Information Commissioner's Office

Call for evidence:

Age Appropriate Design Code

Start date:27 June 2018
End date: 19 September 2018

ico.
Information Commissioner's Office

This response has been prepared by the project, *Children's data and privacy online: Growing up in a digital age (*[redacted]. The project is funded by the ICO and conducted at the Department of Media and Communications, London School of Economics and Political Science. See http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline

Section 1: Your views and evidence

Development needs of children at different ages

The Act requires the Commissioner to take account of the development needs of children at different ages when drafting the Code.

The Commissioner proposes to use their age ranges set out in the report Digital Childhood – addressing childhood development milestones in the Digital Environment as a starting point in this respect. This report draws upon a number of sources including findings of the United Kingdom Council for Child Internet Safety (UKCCIS) Evidence Group in its literature review of Children's online activities risks and safety.

The proposed age ranges are as follows:

3-5
6-9
10-12
13-15
16-17

Q1. In terms of setting design standards for the processing of children's personal data by providers of ISS (online services), how appropriate you consider the above age brackets would be (delete as appropriate):

Quite appropriate

Q1A. Please provide any views or evidence on how appropriate you consider the above age brackets would be in setting design standards for the processing of children's personal data by providers of ISS (online services)

This consultation response is based on the rapid evidence review undertaken as part of the project Children's data and privacy online: Growing up in a digital age. The evidence review included a comprehensive search of 19 databases (yielding 9,119 search results) and an expert consultation (adding further 270 results) followed by an analysis of the most relevant empirical studies (130). Key empirical studies are summarised in Appendix 1. The methodology for the evidence review will soon be published at http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline

The review examined empirical studies with children relating to privacy, personal data and the digital environment. We detail findings below as they relate to age, where such information is available. The recommendations are based on the project findings, as well as on suggestions made during an expert consulation held at the London School of Economics and Political Science (LSE) in September 2018.[1]

In overview, and overwhelmingly, the evidence documents children's struggles with and lack of digital literacy or understanding regarding the uses of their personal data in the digital environment. This is not necessarily for want of interest or ability. Rather, the evidence is clear that children cannot – and cannot be expected to – understand sufficiently many of the ways in which their data is used, or for what exactly their consent is formally required by an online provider. This is for multiple reasons, including the complexity of the digital interface presented to a child, usually written in complex language etc. It is also because often no real choice is attached to a decision about providing personal data or choosing how one's data are used – if there is no choice but the "take it or leave it" choice to provide data to use a service or not to access the service, children will generally not find the "choice" offered meaningful or worthy of consideration. Further, it is because the uses of personal data concern not only the intent and actions of the online provider but also the digital ecosystem that lies behind them– of data brokers, profiling companies, algorithms combining and calculating across data sets, to service the businesses of many players beyond that initially collecting data from a child: the UK does not teach its children about this commercial (and state) ecosystem and thus cannot reasonably expect children of any age to understand it.

It is likely that everything stated in the previous paragraph also applies to the majority of the adult population; we recognise this, though do not document evidence relevant to adults here. Nonetheless, we consider it irrelevant to a fair and appropriate treatment of children and their personal data by ISS. The fact that the evidence shows that all children,

[1] For further details on the expert meeting see: http://blogs.lse.ac.uk/mediapolicyproject/2018/09/17/could-hide-by-default-be-a-solution-to-online-privacy-concerns-for-children/

from 0 to 18 years old, insufficiently understand how their data are used by ISS is in our view sufficient to conclude that they all merit treatment that recognises and respects their "best interests" and age-specific needs and rights.

Beyond this, we emphasise that 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 five and fifteen, 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.

Nonetheless, insofar as ISS find it convenient to treat children according to age groups, and insofar as the ICO needs develop an age-appropriate Code (as we greatly welcome), 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/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.

Last we note that privacy, being generally classified as a protection right in the UNCRC, invites protectionist policy and practice responses. While children indeed need protection from misuses and abuses of their privacy and personal data, the evidence repeatedly shows that efforts solely devoted to protecting children can inadvertently or inappropriately reduce their positive rights to provision and participation, including in the digital environment. Given this, it is important also to recognise that privacy plays a crucial enabling function – privacy brings autonomy, identity and agency, and is vital also for children to benefit from the opportunities of the online world. It is therefore important that the Code does not legitimise undue restrictions either on children directly or on the services that could provide for them.

Beyond these general remarks regarding the evidence and the question of age groupings asked above, our findings suggest the following:

- Current evidence on children's privacy concerns, risks, and opportunities utilises a range of age brackets and applies them inconsistently. A large number of studies focus on 12-18 year olds, paying much less attention to younger cohorts. **Studies rarely disaggregate findings amongst the different age groups** (Livingstone et al., 2018b).

- 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 (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 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).

- While childdren 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 socioeconomic status (SES) home (DE) might have similar knowledge and digial literacy as a 11-year old from a high SES home (AB), as we show here (Livingstone et al., 2018a).

- **Data and evidence pertaining to design standards and regulatory frameworks based on disaggregated age groups are low** and merit further investigation. Age-appropriate app or platform advisories, for example, must account for children's knowledge and abilities - apps advising 'ages 3+' that include in-app purchases and advertisements may be beyond a younger child's abilities and knowledge. Younger age groups will require additional standards or consideration when designing app permissions.

Q2. Please provide any views or evidence you have on children's development needs, in an online context in each or any of the above age brackets.

- **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, sexual exploration (Raynes-Goldie and Allen, 2014; Peter and Valkenburg, 2011)

- **Online platforms provide opportunities for development** (while also introduce and amplify risks) that children can use to build the skill entourage that they need for their growth.

- There is also solid evidence that **understanding of privacy becomes more complex with age** and that the desire for privacy also increases (Kumar et al., 2017; Chaudron et al., 2018).

- Our findings suggest that **children are primarily aware of data given in interpersonal contexts**. 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 digital age. Yet there are gaps in our knowledge of how children experience institutional privacy, raising questions about informed consent and children's rights (Livingstone et al., 2018b). 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 suggests that commercial privacy is the area where children are least able to comprehend and manage on their own (Livingstone et al., 2018b).

- Due to the nature of the existing research, it is difficult to provide evidence in each of the identified age brackets. **Most of the available evidence involved children aged 12+**.

- Based on the comprehensive systematic evidence mapping we identified three groups of evidence (see table 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 identified by the ICO.

Table 1: Mapping child development and privacy online

Age	Evidence on child development
5-7 years	• There is limited evidence on children's understanding of privacy for the youngest age groups but the existing evidence suggests 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, 2017). • Existing empirical studies highlight that 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). • Children are confident internet users but 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). 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 harder 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 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 tracking their devices or monitoring of their activities as a cause for concern or breach of privacy (Gelman et al., 2017).
8-11 years	• Over one in five UK children aged 8-11 (21%) have a social media profile (Ofcom, 2017)even though they are officially below the required age to use these platforms • Children 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, 2017).

- Children associate privacy risks mainly with 'stranger danger' (Raynes-Goldie and Allen, 2014; Children's Commissioner for England, 2017a).
- They start to understand that sharing can create some risks for them (Kumar et al., 2017).
- They still have gaps in understanding privacy terms and conditions which are unclear and inaccessible to them
- Their approach to privacy management is based on rules and not internalized behaviour, hence they find it hard to apply their knowledge to practical situations (Kumar et al., 2017). However, children 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 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).
- Interactive learning is shown to improve awareness and transfer to practice at this age (Zhang-Kennedy et al., 2017).

12-17 years

- The older children become, the more actively they use the internet and the more technical skills they acquire. For example, 46% of UK children aged 12-15 years know how to ever 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) (Ofcom, 2017). These technical skills, however, are not necessarily paired with good knowledge of privacy risks nor 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 different platforms (Xie and Kang, 2015).

- At this age children are not unaware of privacy risks: they engage in a careful consideration of information disclosure (Wisniewski et al., 2015) and balance their desire to protect themselves with the need to participate and socialise (Third et al., 2017; Betts and Spenser, 2016). 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). Their decisions are also based on their partial understanding of the nature and operation of the internet and its uses of personal data.

- 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 (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, removing content, tags or withdrawing from the internet, managing privacy settings or friendship circles (Almansa et al., 2013; Livingstone, 2008; Mullen and Hamilton, 2016;

Emanuel and Fraser, 2014).

- 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). Feeling in control of their data makes children more vulnerable to sharing personal information (Emanuel and Fraser, 2014).

- Children of this age see the online environment as their 'personal space' for self-expression, socializing and they are often concerned about parental intrusion of their privacy (boyd and Marwick, 2011; Martin et al., 2018; Redden and Way, 2017).

- They have a good understanding of online restrictions and monitoring by the school (Cortesi et al., 2014) – for example, they know their online activities when using a school computer are monitored and the content they can access is restricted.

- Children demonstrate awareness of the 'data traces' they leave online (e.g. in relation to seeing advertisements following their earlier searches) (Zarouali et al., 2017) and device tracking (e.g. that some apps use their geo-location) (Redden and Way, 2017) but find it hard to make personal connection - how their data is being collected and to what effect (Acker and Bowler, 2018; Emanuel and Fraser, 2014).

- Children even at this age 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 (Bowler et al., 2017).

- At this age privacy risk functions mostly as a 'learning process' – children are mostly engaged in retrospective behaviour trying to rectify past and hold expectations that they are able to retract their online activities (Wisniewski et al., 2015; Wisniewski, 2018).

- Privacy-related media literacy education can increase children's awareness of technological solutions or tighter privacy settings as coping and threat-mitigating strategies (Youn, 2009). However, 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, 2018; Wisniewski et al., 2015).

Our recommendations

- Online service providers must be required to show how they take the best interests of children into account (e.g. under what circumstance can sharing personal data be the best interest of a child?). Since 1/3 people on the internet are under 18, this is surely a sufficient market such that meeting children's interests is a commercial proposition.
- Automated data collection, such as collection of geo-location, should be turned off by default for children under 18.
- Industry must work together to make data collection and privacy protection look familiar to people, without them having to read terms and conditions to understand the general settings (especially important for children who have little awareness of the consequences of data sharing). This does not mean abandoning each company's own branding or strategies, but it is about establishing a "labelling infrastructure" (like traffic signals) that indicates the level of privacy on offer and provides proper environment online for children.
- "Rights by design" is vital so a child could check, contest, rectify, erase or edit information about themselves - similar systems exist for editing profiles and or inferences (such as Google's ad management page).
- The list of design features identified in the consultation document should be considered seriously, asking the question – what does a child need online? An argument can be made for the highest privacy settings by default, collecting personal data only for a good reason, upholding

terms and conditions.

- It is significant and should be commended that the Data Protection Act explicitly mentions the UNCRC, especially the importance of ensuring the best interests of all children under 18 years old. The best interests of the child should be the key question to answer in any systematic design of services.
- The principle of data minimalisation is crucial. Data must be service-critical, and that does not include sharing with third parties.

The United Nations Convention on the Rights of the Child

The Data Protection Act 2018 requires the Commissioner to take account of the UK's obligations under the UN Convention on the Rights of the Child when drafting the Code.[2]

Q3. Please provide any views or evidence you have on how the Convention might apply in the context of setting design standards for the processing of children's personal data by providers of ISS (online services)

The United Nations Convention on the Rights of the Child (CRC), (1989) establishes the basic standards that apply without discrimination to all children worldwide and specifies the minimum entitlements that governments are expected to implement. The CRC is now being debated and actively applied in relation to digital domains and activities. We have tried to map the CRC child rights onto areas related to privacy design standards (see Table 2 below).

[2] The table is based on Livingstone, S. (2016) *A framework for researching Global Kids Online: Understanding children's well-being and rights in the digital age.* London: Global Kids Online. Available from: www.globalkidsonline.net/framework

Table 2: Mapping child rights onto privacy-related design standards

United Nations Convention on the Rights of the Child (CRC) *(articles selected and paraphrased)*	**Application of the CRC to setting privacy-related design standards** *(indicative topics)*
Protection against all forms of abuse and neglect (Art. 19), including sexual exploitation and sexual abuse (Art. 34), and other forms of exploitation prejudicial to the child's welfare (Art. 36). Protection from 'material injurious to the child's well-being' (Art. 17e), 'arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation' (Art. 16) and the right of the child to preserve his or her identity (Art. 8).	Web design, interface, and functionality should not facilitate children's negative experiences and risks – businesses should implement design, self-regulation, and redress aiming to prevent and reduce children's exposure to possible harms in a range of areas related to children's rights. For example: • Businesses and design standards should aim to prevent the use of children's data (by anyone) for purposes of sexual grooming, sexual exploitation and abuse. • Businesses and design standards should aim to prevent the use of children's data for the creation and distribution of child abuse images. • Should aim to block online dimensions of child trafficking. • Should aim to stop the use of children's data for exposing minors to (diverse, extreme, illegal) pornography. • Should aim to prevent personal data exploitation, misuse, unwarranted sharing or tracking in digital environments. • Should avoid design facilitating or insufficiently redressing hostility, hate, harassing and bullying content, contact and conduct online.

	• Should avoid design facilitating or insufficiently redressing threats to dignity, identity and reputation online. • Should avoid design facilitating or insufficiently redressing threats to privacy via exposure to institutionalized or commercial use of children's personal data. • Should avert the use of children's data for inappropriate information and persuasion regarding self-harm, violence, suicide, pro-anorexia, drugs.
Provision to support children's rights to recreation and leisure appropriate to their age (Art. 31), an education that will support the development of their full potential (Art. 28) and prepare them 'for responsible life in a free society' (Art. 29), and to provide for 'the important function performed by the mass media' through diverse material of social and cultural benefit to the child (including minorities) to promote children's well-being (Art. 17).	• Businesses, design standards, and regulators should seek to facilitate the availability and distribution of formal and informal age-appropriate learning resources and curricula about personal data and privacy online. • Businesses, design standards, and regulators should aim to give children access to wealth of accessible and specialised information related to privacy online. • They should aim to provide opportunities for creativity, exploration, expression online and with digital media in a way that does not compromise children's privacy online. • They should design aiming to develop digital, critical and information skills and literacies related to both the internet as a whole and to privacy online in particular. • They should aim to provide digital means to counter or circumvent privacy-related inequalities or to address special needs.

	• They should aim to offer an expanded array of age-appropriate entertainment and leisure choices online without compromising children's privacy. • They should provide opportunities for access to/ representation in/ response to content relating to own culture, language and heritage without compromising children's privacy.
Participation: this includes the right of children to be consulted in all matters affecting them (Art. 12); also, the child's right to freedom of expression (Art. 13) and to freedom of association (Art. 15).	• Businesses, design standards, and regulators should aim to enable the take up of enhanced connections and networking opportunities in a way that does request the provision of personal data in exchange for access. • Businesses, design standards, and regulators need to provide opportunities for consulting children about governance including in relation to data protection and online privacy. • They should provide user-friendly fora for child/youth voice and expression regarding privacy online. • Businesses and design standards should offer design solutions fostering peer-to-peer connections for entertainment, learning, sharing and collaboration that do not infringe children's data protection rights. • Providers of online services likely to be accessed by children need to base their designs on the recognition of and provision for child/youth rights, responsibilities and engagement online.

Aspects of design

The Government has provided the Commissioner with a list of areas which it proposes she should take into account when drafting the Code.

These are as follows:

- default privacy settings,
- data minimisation standards,
- the presentation and language of terms and conditions and privacy notices,
- uses of geolocation technology,
- automated and semi-automated profiling,
- transparency of paid-for activity such as product placement and marketing,
- the sharing and resale of data,
- the strategies used to encourage extended user engagement,
- user reporting and resolution processes and systems,
- the ability to understand and activate a child's right to erasure, rectification and restriction,
- the ability to access advice from independent, specialist advocates on all data rights, and
- any other aspect of design that the commissioner considers relevant.

Q4. Please provide any views or evidence you think the Commissioner should take into account when explaining the meaning and coverage of these terms in the code.

- **Default privacy settings**: there is substantial evidence that children of all age groups do not understand fully privacy online, especially in relation to institutional and commercial use of their data (Steijn and Vedder, 2015; Livingstone et al., 2018b; Livingstone, 2008). Child-friendly default privacy settings can protect children who are less able to comprehend what they are agreeing to. Research also shows that shifting defaults privacy settings makes it difficult for children to maintain a consistent privacy level, which is heightened by inconsistent levels between different platforms (Bailey, 2015).

Our recommendations

- Unified location (or, at least, findability) and look (recognisability) of privacy settings across child-facing products and services is crucial.
- Moving responsibilities (to manage privacy and personal data) from children/parents/teachers to online service providers in necessary,

since evidence shows it is unfeasible to expect children to sufficiently understand the privacy implications of a complex digital environment, or to expect them to be resilient in an environment which does not provide adequately (or, sometimes, at all) for their developmental needs.

- Making "default" settings better: switching data harvesting a profiling off by default can ensure that children's personal data is protected more efficiently, including for children who do not know how to change their settings.

- **Data minimisation standards**: existing research with children also suggests that they want to be in control of their personal data and make decisions about what is shared (boyd and Marwick, 2011; Agosto and Abbas, 2017). Application design and interface can influence children's decisions to share information that they would not volunteer otherwise – even older teens might agree to data sharing just to be able to use a service or product, being curious or wanting to take part in something that their friends do; or they might provide information online when prompted to without realizing that they could skip this step (Bailey, 2015; Chi et al., 2018; De Souza and Dick, 2009).

Our recommendations

- Data minimization by default will help ensure that less personal data is collected or shared without the full understanding or consent by children. It will also reduce the fake 'voluntary' data sharing by children.

- **The presentation and language of terms and conditions and privacy notices**: in their current form terms and conditions are hard to understand even for the older children (12-17) (Coleman et al., 2017). Research with children has shown that they would like to engage more with the terms and conditions but these need to be shorter, clearer, accessible, and in more attractive and accessible audio or video form (Coleman et al., 2017).

Our recommendations

- Shorter, clearer, and more accessible (audio or video) terms of use: ease of use, ubiquitous functions and user-friendly features of the privacy presentation and language may reinforce children's privacy protection behaviours.

- **Uses of geolocation technology**: geo-location technology is used in a number of games and social media apps that children use. The evidence suggests that both younger (8-11) and older (12-17) children seem to have an understanding of how apps record their movements and can foresee some risks associated with this (Redden and Way, 2017; Raynes-Goldie and Allen, 2014; Ghosh et al., 2018) but the risks that the younger children envision are mainly related to being identified or contacted by strangers (Raynes-Goldie and Allen, 2014). While older children have a more comprehensive relationship with geolocation tracking and like to be in control of how their location data is shared, where and with whom (Redden and Way, 2017) but many still share their location by default (e.g. 16% of 12-17 children in the USA; Madden et al., 2013).

- **Automated and semi-automated profiling**: profiling is one of the aspects of commercial and institutionalized privacy that children struggle to comprehend – in terms of its mechanisms, purposes, and consequences (Livingstone et al., 2018b).

Our recommendations

- A design solution is vital which makes profiling comprehensible to children, identifying what kind of data is profiled, how and to what ends, using clear 'real-life' examples that children of different ages can relate to.

- Improve privacy control navigation: enable granular control over privacy settings (with defaults switched off) to match the elaborate data-harvesting techniques and create better industry standards around user empowerment.

- Design standards should allow the full profiling control and its easy navigation to respond to children's individual needs for independence, anonymity and connectivity.

- **Transparency of paid-for activity such as product placement and marketing**:

The significant purchasing power that children wield within their families has led to their emergence as a consumer segment of interest for marketers and especially so online. Cookie-placement, location-based advertising, and behavioural targeting are used by marketers to collect personal information from children to reach and appear to this target audience (Shin and Kang, 2016). The evidence suggests that younger children (under 12) sometimes struggle to identify commercial content due to its similarity to other web or app content and can remain oblivious to being the targets of commercial activity (Ofcom, 2017). Older teens (16-19) have a better understanding of how personal data can be used to target commercial content, which for some is causing privacy concerns (Xie and Kang, 2015; Zarouali et al., 2017; Acker and Bowler, 2018). Nevertheless, even older teens are affected by paid-for activities and are shown more likely to purchase products after seeing targeted advertising (Zarouali et al., 2017). Across the age spectrum, children report being bothered by unwanted content such as internet scams and pop-up advertisements (Byrne et al., 2016).

Our recommendations

- 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 children's age. Transparency and age-verification are needed to redress these issues.

- **The sharing and resale of data**: our pilot research with children of different ages shows that they struggle to understand their activities in terms of data and often think that what they do is insignificant and of no interest to commercial entities (Livingstone et al., 2018b). Even teens (12-18) who have varying interpretations of the nature of online data and only a broad understanding of the lifecycle of data, with most finding it difficult to connect with data at a concrete and personal level, with the notion of a personal data dossier either non-existent or abstract (Bowler et al., 2017). They have little knowledge of data flows and infrastructure and while aware of the security issues related to online disclosure of personal data, they are struggling with the notion

of digital traces of their data and to envision any possible implications for their future selves (Bowler et al., 2017).

Our recommendations

- The design need to clarify the type and mechanisms of data sharing in a comprehensible way and to flag up future potential risks.
- Sharing and resale of data needs to be disabled by default as most children struggle to understand and consent to it and should be made available only via parental verification.
- Children's choices should be real and granular so that children are not forced to consent to gain access to a service.

- **The strategies used to encourage extended user engagement**: children often regard official business language uncritically – when they are told that something is done to improve their use experience, they believe that this is the (only) purpose. Such misunderstandings can create a false sense of security and trust, which then makes children more vulnerable to disclosure of sensitive information due to minimisation of perceived risks. Our pilot research shows that covert user engagement strategies are hard to comprehend but impactful on children's choices and behaviours and need to be made explicit to child users. More evidence in this area is also needed.

- **User reporting and resolution processes and systems**: child rights considerations should be incorporated into all appropriate corporate policies and management processes (ITU and UNICEF, 2015) including systems of reporting content and providing resolutions.

- **The ability to understand and activate a child's right to erasure, rectification and restriction**: the evidence suggests also that children participate online with the expectations to be able to retract and rectify their activities (Wisniewski et al., 2015). Learning from experiences, including mistakes, is demonstrated to be the most effective way of building resilience and privacy-related media literacy (Wisniewski et al., 2015). At present, however, children face challenges in trying to erase their online presence (for example due to forgotten passwords and lack of access to old accounts). The concept

of "the right to make a mistake" is crucial to think of children as explorers who lack some fear of consequences, and who are better than parents in bypassing the controls (Coleman et al., 2017).

Our recommendations

- Children expect to be able to rectify their online past and erase the traces of unwanted activities. Being able to make mistakes, including online, is part of child development and needs to be an easily accessible and uncomplicated feature of any online service.

Q5. Please provide any views or evidence you have on the following:

Q5A. about the opportunities and challenges you think might arise in setting design standards for the processing of children's personal data by providers of ISS (online services), in each or any of the above areas.

- **Intersectionality and multiplicity**: Age is important in differentiating how ISS should treat children's data, but it is only a starting point, nonetheless. A better understanding of what personal and environmental influences contribute to children's effective management of their privacy online would facilitate a more efficient approach to privacy literacy. Other important factors to consider in addition and in relation to age include gender, vulnerability, first language spoken, disability or special educational needs. Children's privacy should be seen as integral to their social, cultural, economic, developmental and digital contexts – in short, to their wellbeing and life outcomes.

Our recommendations

- Building a more complex approach which includes age amongst other factors will be better suited to address children's specific needs and vulnerabilities.
- Similarly, privacy should not be seen as individual-based but needs to be considered in relation to its social and digital dimensions, as well as in relation to institutional and commercial use of data.

- **Age-appropriateness**: there can be significant differences amongst children of the same age – age ranges are more fluid rather than fixed.

There are currently few studies on children's privacy online which take a developmental approach, so this makes the identification of suitable age ranges for a Code particularly hard. Particularly significant is the gap related to the age group of 12-14-year-old which is crucial because children reach puberty in that period but very little is known about their online privacy practices and experiences. In addition, the fast-developing new technologies may mean that age-appropriate design is not necessarily linked to a certain age but more to the type of online engagement. So, verification of age-appropriate designs would have to be an on-going process.

Our recommendations

- 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.

- **Child-inclusiveness**: Children' understanding and practices around privacy are often different from adults' – making decisions 'on behalf of children' can be challenging. 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 recommendations

- A child-focused approach should be adopted by industry and regulators in order to give recognition to children's voices and to facilitate and support their heterogeneous experiences, competencies and capacities. Such approach can also create opportunities of peer-to-peer support and a more inclusive and tolerant online environment.

- **Ensuring participation**: it is important to ensure that safeguarding measures do not lead to restrictions of children's online participation.

Our recommendations

- Age verification included in the Code should be designed not to restrict the access of children but to keep children as participants in a suitable online environment.

- Children should have the opportunity to make real and transparent choices about their data which do not limit their ability to participate. Intent of data collection must be aligned with the best interest of children.
- Allowing safe learning by doing - incorporating digital literacies and skills into the architecture and design of platforms and building children's privacy-related digital competencies (in addition to others) as they use and engage with digital platforms and devices.

- **Working in partnerships**: the initiative might face industry opposition to offering better standards of services to children. Cross-national differences in regulations is likely to create further challenges.

Our recommendations

- Working collaboratively and closely with industry partners for creating a sense of shared ethical responsibility for delivering high-quality services to children is needed. In relation to the context of design concept, "dark patterns" and "good patterns" of online use should be distinguished and called out.
- Location of responsibility should lie within the industry, rather than children, their parents and educators.
- Establishing clear privacy ratings that both businesses and users understand and use as a standard to guide practice will be widely beneficial.
- The focus should fall on the overall design of online environment and its ecology, rather than enforcement of regulatory measures.
- Managing the potentially international reach of the Code should involve consultations and collaborations with the rest of the world.
- Working across the landscape of child regulation to allow for consistency and transferability of principles and language is essential.

Q5B. about how the ICO, working with relevant stakeholders, might use the opportunities presented and positively address any challenges you have identified.

Q5C. about what design standards might be appropriate (i.e. where the bar should be set) in each or any of the above areas and for each or any of the proposed age brackets.

Q5D. examples of ISS design you consider to be good practice.

Q5E. about any additional areas, not included in the list above that you think should be the subject of a design standard.

Q6. If you would be interested in contributing to future solutions focussed work in developing the content of the code, please provide the following information. The Commissioner is particularly interested in hearing from bodies representing the views of children or parents, child development experts and trade associations representing providers of online services likely to be accessed by children, in this respect.

Name: [redacted]

Email: [redacted]@lse.ac.uk

Brief summary of what I can offer:

My expertise is in the field of children's data and privacy online, internet opportunities and risks for children and young people, media literacy, and media regulation. See [redacted]

Further views and evidence

Q7. Please provide any other views or evidence you have that you consider to be relevant to this call for evidence.

Setting age labels and content descriptors to demarcate un/suitable content

The PEGI- Pan-European Game Information- group sets age labels and content descriptors to indicate if content is suitable for the end-user. Since 2012, PEGI is the only system used in the UK for console and PC games. In the UK, PEGI 12, 16, and 18 ratings are legally enforceable.

For smartphones and tablets, PEGI uses six age categories (3+, 7+, 12+, 16+, 18+) and eight content descriptors[3], in addition to a 'Parental

[3] 1) May encourage or teach gambling, 2) May be frightening to younger children, 3) Contains the use or glamorisation of alcohol and/or drugs, 4) contains depictions of nudity and/or references to sexual behaviour, 5) can only appear on games rated 18 containing depictions of ethnic, religious,

Guidance Recommended' tag. The guidance recommendation is also used for non-game apps such as Facebook or YouTube to flag the user-generated or content-curation that occurs on these platforms.

UKCCIS (2015) advises social media and interactive services providers to pay special attention to children under the age of 13 (building on COPPA, given many providers are US-based). They differentiate between content risk (age-inappropriate information), conduct risk (in an interactive situation where their or others' behaviours may put them at risk), and contact risk (being vulnerable or victims due to their online interactions); in addition to commercial risks (advertising). These may also work as warnings or advisories and may be design or regulatory settings to consider.

nationalistic or other stereotypes that could encourage hatred, 6) Contains bad and / or offensive language, 7) Contains depictions of violence, and 8) Can be played online.

Section 2: About you

Are you:

A body representing the views or interests of children? Please specify:	☐
A body representing the views or interests of parents? Please specify:	☐
A child development expert? Please specify:	☐
A provider of ISS likely to be accessed by children? Please specify:	☐
A trade association representing ISS providers? Please specify:	☐
An ICO employee?	☐
Other? Please specify: Academic research project.	☒

About the authors

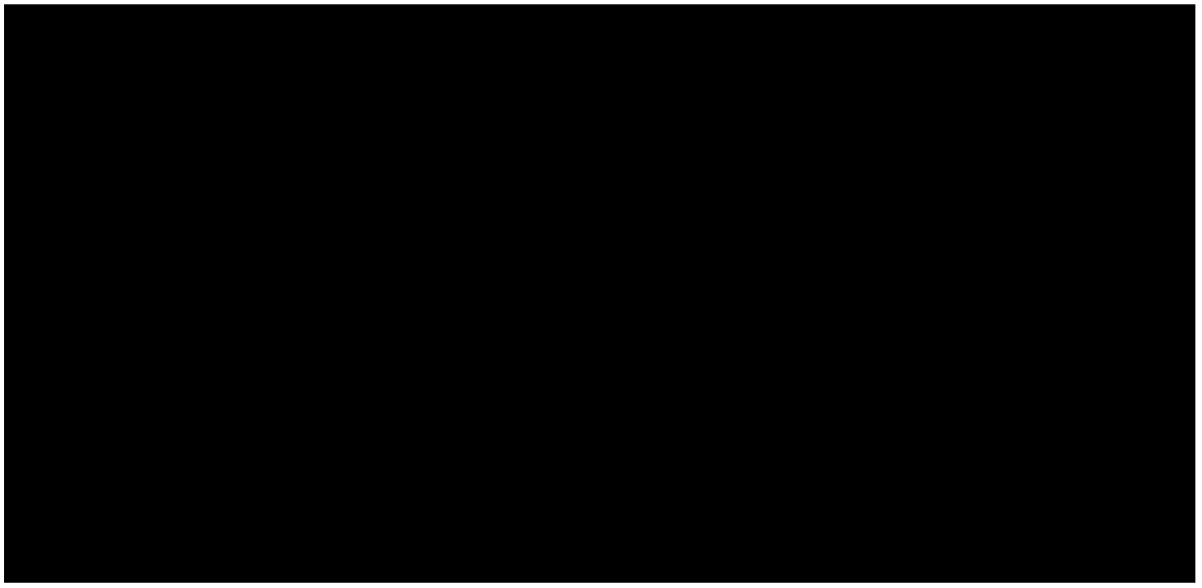
This response has been prepared by the project, *Children's data and privacy online: Growing up in a digital age.* The project is funded by the ICO and conducted at the Department of Media and Communications, London School of Economics and Political Science. See http://www.lse.ac.uk/media-and-communications/research/research-projects/childprivacyonline

Contact details: (tel.) [redacted] (email): [redacted]@lse.ac.uk

The research team is as follows:

[redacted]

[redacted]



Appendix 1: Summaries of key empirical studies

1. Abbas R and Mesch GS. (2015) Cultural values and Facebook use among Palestinian youth in Israel. *Computers in Human Behavior* 48: 644-653.

Age: 16-19 [categorised as: 12-15, 16-19]
Privacy Type: interpersonal
Data Type: data given
Method: ex-post facto
Country: Israel (Palestinians in Israel)
Study Focus: attitudes and beliefs, decision-making.
Platform: Social networking sites

The existing literature and theory (e.g use and gratification theory) on social media use explains platform engagement is driven by desire for information, friendship and communication, and is shaped by the user's social status and positioning, dispositions, gender and age. The authors focus on the importance of cultural values and explore the influence of factors such as uncertainty avoidance, collectivist values, the strength of social hierarchies (power distance), privacy concerns and trust on Facebook use to maintain and expand social ties. Authors draw on Westin (1967) to conceptualise privacy as decisions regarding when, how, and to what extent information about the individual is communicated to others.

Privacy concerns are measured via an 11-item 5-point Likert scale (from 'never' to 'always', based on Buchanan et al. (2007) (items include: "I am concerned about my privacy when using a Facebook account", "I am concerned about online organizations not being who they claim they are", and "I am concerned about online identity theft"). Trust is measured via a 4-item 5-point Likert scale adapted from Pan and Zinkhan (2006) (items include: "Facebook's site can be trusted", "I can count on Facebook to protect my privacy", "I can count on Facebook to protect customers' personal information", and "Facebook can be relied on to keep its promises").

OLS regression was used to test the association between attitudes about trust and privacy concerns and cultural values. The study found a significant positive relationship between "traditional cultural values" (high collectivism, power distance and uncertainty avoidance) and the motivation for using Facebook for maintaining existing relationships, even when controlling for trust and privacy concerns. Collectivism and power distance were also associated with high trust in Facebook and expanding social ties, where also gender differences were observed – more boys than girls reported using Facebook to expand their social ties, while more girls reported privacy concerns. Trust in Facebook is associated with higher maintenance and expansion of social ties but the more users use Facebook to expand their ties, the more concerned they are about their privacy. The authors refer to existing studies which provide some

evidence that more individualistic cultures are associated with higher concerns about privacy but their own study found the opposite – higher collectivism was associated with more privacy concerns.

Note: These results differ from other studies cited in the text which focus on social media more generally (e.g. others show a negative association of power distance and social network adoption and collectivism and privacy concerns).

2. **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.**

Age: 11-17 [categorised as 8-11, 12-15, 16-19]
Privacy Type: commercial
Data Type: data traces
Method: participatory
Country: USA
Study Focus: data literacy
Platform: Social networking sites

Using data-literacy workshops ("Data Silhouettes") for young people 11-17 (n=24), the authors explore young peoples' understanding of their data worlds. The authors share preliminary findings from piloting a library-based learning experience to explore the links between social media behaviour and data traces. Interviews reflected young peoples' concerns about privacy but showed that they lacked a concrete link between social media networks and personal data, where they viewed data as similar to a "black box". However, respondents also understood and viewed their data as a part of their personal identity, yet rarely mentioned privacy or safety in relation to it.

The study draws on Marchionini (2008), who refers to these data traces as "proflections of self"- data traces of interactions created un/consciously that make up our collective, virtual selves. Authors contextualise data literacy within personal data management, allowing young people to work towards the analytical skills needed to curate and obfuscate their data lives.

3. **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.**

Age: 11-18 [categorised as: 8-11, 12-15, 16-19]
Privacy Type: commerical, interpersonal
Data Type: traces, given

Method: interviews
Country: USA
Study Focus: data literacy
Platform: Social networking sites

This study explores American teens' understanding of "data" in the context of social and mobile media. Draws on interviews with 11-18 year olds (n=22) to explore their understandings and perceptions of data literacy, and their knowledge acquistion.

Teen lives are saturated with technology that is pervasive, portable, and persistent. Traditional understandings of the data lifecycle are disrupted by mobile computing and wireless devices. The authors argue that young peoples' data worlds are influenced by their use and ownership of mobile devices. Preliminary findings suggest that respondents view data as "numbers". Some older respondents, however, described data as numerical representations of information in documents or reports. Data are also thought of as access to internet through web-browsing or social media applications, data plans, or data as access to rich-internet content. Younger respondents struggled with distinguishing between accessing mobile broadband and switching between home or public wi-fi networks. In discussions on data traces, responses suggest that young people think of data as easily spread and public-facing, collected by government or advertisers. Older teens described ad-targetting on platforms based on their use, connecting it to their sense of self/online personas. Respondents were aware that apps and online services can access their location information or other data, but did not apply privacy or rights lenses to it.

4. **Ahn J, Subramaniam M, Fleischmann KR, 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.**

Age: "middle school" (doesn't specify age groups) [categorised as: 11-13]
Privacy Type: interpersonal
Data Type: Data given
Method: participatory
Country: USA
Study Focus: attitudes and beliefs
Platform: Online platforms- remixing, sci-identity.org

In this participatory case-study conducted across four inner-city schools in the USA, the authors worked with school librarians on an after-school program focused on science storytelling and developing students' identities as scientists and engineers (sci-dentity.org).

Young people are active creators of information, utilising digital tools to remix and copy previous work; raising questions of appropriation, copyright, privacy, and information literacy. This paper, using a case study of a hybrid online and offline community of middle school students, illustrates the complex issues that arise when youths remix, share, and adapt their peers' media artefacts. Remix is an information behaviour and (digital) literacy skill learnt over time, and a part of "participatory culture" (Jenkins, 2009)[4]. Authors consider how young people, as information literate individuals, "identify with (a) attitudes towards information appropriation, (b) strategies of remix, and (c) the underlying values that motivate their ideas about remix practices".

In terms of privacy values, students emphasised the need to acknowledge contributions and the mechanisms for credit but acknowledged that it raised privacy concerns: requiring account creation, making online activities traceable, and making online identities visible to others. Their participation in these communities or platforms is valued over privacy, and when given options to enact privacy controls; they chose not to do so. In this study, even though explicitly afforded the option to create anonymous profiles, students chose not to do so.

5. 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: 127-134.

Age: 12-15 [categorised as 12-15]
Privacy Type: interpersonal
Data Type: data given
Method: Mixed methods (interview, content analysis)
Country: Colombia and Spain
Study Focus: behaviours, media literacy, privacy strategies used
Platform: SNS
Other existing studies on social media and privacy focus on the security risks but the authors aim to offer a more balanced view of social media, exploring how young people use social media as a source of communication. The authors found that young people are generous with the personal information they share online – more so in Spain than in Colombia. Youth manage their identity via their Facebook profiles; carefully selecting and staging the profile pictures they post. Yet, about a third of the profiles contained personal information, such as birthdays, address, school, as well as favourite activities, music, films; and about a fifth contained relationship information. This information was not always

[4] Jenkins H. (2009) *Confronting the challenges of participatory culture: media education for the 21st century,* Cambridge, Mass.: Cambridge, Mass.: MIT Press.

correct – some give an earlier date of birth, others stated they were married. Adding unknown people as friends was not uncommon.

Note: This is primary research with mixed-method analysis (40 interviews with young people aged 12-15 and content analysis of 200 Facebook profiles). The study makes generalised statements based on a small sample.

6. Aslanidou S and Menexes G. (2008) Youth and the Internet: Uses and practices in the home. *Computers & Education* 51: 1375-1391.

Age: 12-18 [categorised as: 12-15, 16-19]
Privacy Type: interpersonal
Data Type: data given
Method: Survey
Country: Greece
Study Focus: media literacy, behaviours
Platform: General

In this study, students from 17 schools (12-18 years old. N=418) in four Greek cities completed a self-reported questionnaire on Internet use at home, and types of parental supervision (in 2004-2005).

Authors found that internet access remains low and is an indicator of SES stratification. It is insufficiently used for school purposes but younger students (12-15) used it more frequently for school work than their older counterparts. The Internet is considered a personal space for action and expression that they preferred using or surfing alone, and where they can safeguard their privacy. A significant percentage, however, also reported that they very often or always used it with their friends. Parental supervision and monitoring of their internet use is largely absent, and largely concerned time spent online and monitoring/controlling online purchases.

7. 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: 2645-2664.

Age: 8-19 [categorised as: 8-11, 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: survey
Country: UAE
Study Focus: behaviour, support-guidance, attitudes and beliefs
Platform: SNS (a range)

The authors utilised an online survey tool to gather data from private and

public schools in the UAE (grade 6 and above, n=31,109- 59% girls, 41% boys). The online survey explored students' reasons for joining social networking sites, parental knowledge of activities and their chances of being invited to join children's social networking groups.

Mobile phone and Tablet PC usage was more prevalent than other devices, and students spent on average 5.2 hours/day on online social networking. The survey listed 27 online social networking applications, and respondents noted whether they had an account. The top 11 items were (in order): Facebook, Twitter, Google Plus, Tumblr, Instagram, Ask.fm, Skype, SnapChat, YouTube, WhatsApp and Kik. Students were given seven reasons to choose why they used these SNS- the two responses with the highest mean were: (i) "to keep in touch with family and friends", and (ii) "to find information". Students (8.3%) who said they did not use online SNS, were given six reason choices to select from- the two highest were lack of interest, and 'face-to-face communication is preferred in my culture". There were gendered differences recorded for use and non-use. Girls, in particular, gave higher scores (on non-use) to "my parents do not allow me to use it", "I have privacy concerns", and "face-to-face communication is preferred in my culture". There were also differences by grade (or age)- as they get older, their reasons for (non-) use are different. In particular, as they get older, the mean scores for lack of interest in SNS and privacy concerns were greater.

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

Age: 15-17, 18-22 [categorised as: 12-15, 16-19]
Privacy Type: institutional
Data Type: given, traces
Method: Focus group discussions/ Interviews
Country: Canada
Study Focus: attitudes/beliefs, behaviour**,** interface
Platform: SNS

The authors explore girls (15-17) and young women (18-22)'s perspectives on current technology-related policies in Canada, focusing on amendments to criminal law to address online child pornography, cyberbulling, luring etc. They also investigate young women's experiences with social media, and their perspectives on policymakers' debates.

Findings suggest 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. Participants contextualised their online practices, reflecting on the benefits of online interaction and self-exploration, 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 them.
Participants indicated that the design and architecture of social media sites can create incentives to expand networks and engage in risky online behaviour such as adding or friending strangers. The environments are structured to elicit information disclosure, potentially exposing them to surveillance and judgement. They also indicated that technical architectures can complicate self-help privacy strategies. Complex user agreements and platform architecture may suggest that disclosure of a considerable amount of information is necessary when it is not actually required. Participants also wondered about their data use by online service providers, and the particularities of privacy settings. Participants noted that privacy-setting defaults keep shifting, making it difficult to maintain a consistent privacy level, which is heightened by inconsistent levels between different platforms.
Participants identified that surveillance- as a means of protection- infringes on their rights and privacies too. Suggest that platform providers are regulated to improve privacy controls- data deletion, for example, must be permanent across all systems and spaces; with greater user control over trade/sales of their data to third-parties.

9. Bakó RK. (2016) Digital transition: Children in a multimodal world. *Acta Universitatis Sapientiae, Social Analysis* 6: 145-154.

Age: 4-8 [categorised as 4-7, 8-11]
Privacy Type: interpersonal
Data Type: given
Method: observation, participatory
Country: Romania
Study Focus: digital literacy, attitudes
Platform: General

Uses multimodality concepts, this study investigates how texts are read and produced across a range of platforms and devices by young children, and their related skills and competencies. It explores 4-8 year old children's ICT-use, digital literacy levels, favourite technologies, and attitudes towards ICTs.
Children, through visual methods such as drawing and interacting with tablets in the study process, depicted their family lives as immersed in smart devices. They were confident with navigating online spaces- apps, e-mail, game downloads, and in using tablets; needing little to no guidance. Researchers conclude that children are comfortable with smart device use, experiencing it daily, and are immersed in multimodal technological enviroments. Despite this, they are narrow, routine users who do not fully understanding the opportunities and risks associated with

their online use. These are preliminary results and more in-depth findings and conclusions are forthcoming.

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

Age: 14-17 [categorised as: 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: Observation (online)
Country: USA?
Study Focus: privacy strategies
Platform: SNS

Uses an online observational, ethnographic approach (observing 14-17-year olds' Facebook and Ask. FM profiles through "friends of friends" settings), authors suggest that adolescents engage in strategic privacy management as a tactic to increase social and symbolic capital. They contend that in order to show their peers that they're no longer children, adolescents represent their private lives in public spheres.
Authors apply a relational understanding of privacy, where intimacy is a right rather than a space with specific spatial boundaries. Social networking sites mark various milestones in teenagers' private lives, providing communication platforms where teenagers can make these milestones (or their 'growing up') visible; creating a form of "strategic sociality" where intimacy is developed as a resource for prestige, rather than a surrender of their privacy itself. Intimacies are also seen within an "exchange market" where adolescents bargain and exchange intimate information based on their assessment of its value. These social bonds are used as commodities, which is then extended to individuals. Teenagers' degree of "authenticity" is garnered via the public validation they secure through the public sharing of intimacies; making their privacy itself a commodity.
The article demonstrates that as privacy is viewed as resource- not just one to protect, but as social and symbolic capital- it is embroiled in power struggles and manoeuvres for gaining control. This can be viewed as a means to gain autonomy.

11. Barron CM. (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: 401-413.

Age: 8-12 [categorised as: 8-11, 12-15]
Privacy Type: interpersonal
Data Type: given
Method: interviews, observation (mixed methods)

Country: Ireland
Study Focus: privacy strategies, behaviours,
Platform: mobile phones

Surveillance, globally, is becoming the norm in public spaces designed for children. Mobile phones have brought surveillance and monitoring into the realm of personal relationships, normalising 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. Challenges efforts to create 'risk-free environment' as unrealistic and unachievable. Risk aversion restricts children's play, development, agency, and constrains their exploration of physical, social, and virtual worlds.

This paper explores strategies employed by children in middle childhood (8-12 years, n=60, n girls= 32, n boys=28) to negotiate and resist monitoring and surveillance through mobile phones. There have been significant shifts in how children play and the spaces they play in, where geographical proximity is no longer the predominant organising force (some argue as a result of demographic developments and not misplaced cultural values). Field site was an Irish town classified as 'urban', with several housing development/estates that most children in the area reside in. Estates do not have formal communal seating areas or fixed play equipment. Utilised participatory data collection techniques such as visual photography, participant observation in two single-sex schools and in housing estates over one school year. Photo elicitation group discussions held after photographs were collected and reviewed.

Findings reflect that children in middle childhood play close to their home, where parents rely less on mobile phones and on alternate systems. Some children reported having mobile phones for 'emergencies' but were unsure of what that would constitute and instead recounted specific instances (parents checking or confirming location/movements) lending weight to parents monitoring child in time and space, allowing a feeling of control and minimising risk perception. Children, however, understood the phones as a tool for textual rather than oral communication. Children also employ strategies of negotiations, actively engaged in planning their own movements and in an on-going dialogue to compromise with parents (text instead of call, for example). They also employ strategies of resistance (pretending it was silent, ran out of credit, or had a flat battery, giving false information, deleting texts) to avoid or circumvent monitoring or discovery of rule-breaking (going to a friend's house alone, for e.g.). Texting language- use of specific characteristics or codes in text to form a 'texting language- may be incomprehensible to adults, limiting their ability to comprehend texts even when they're read; allowing a resistance to monitoring.

12. Betts LR and Spenser KA. (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.

Age: 11-15 [categorised as: 8-11, 12-15]
Privacy Type: interpersonal
Data Type: given
Method: focus groups
Country: UK
Study Focus: technology interface, attitudes, behaviours
Platform: General

11-15-year olds report feeling vulnerable as SNS requires relinquishing personal information to fully engage in these spaces. However, some felt that this default expectation of disclosure engendered feelings of their privacy violation. It also meant they wished for greater control over their privacy settings. Participants discussed changing privacy settings but were also aware of the interactional nature- as despite their own privacy settings, others with less stringent settings can make them vulnerable. They also discussed the tension between needing to maintain privacy and yet engage in social media spaces. Despite awareness of potential risks, they continued to use social media as risks were perceived to be low and happening to "other" people. If, however, they did encounter a risk, it would shift how they and used and engaged with platforms.
There was awareness of the permanence and longevity of the Internet and their data use, and its potential for future impact.

13. 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.

Age: 11-18 [categorised as: 8-11, 12-15, 16-19]
Privacy Type: interpersonal, commercial
Data Type: traces
Method: interviews
Country: USA
Study Focus: data literacy, interface, attitudes
Platform: General

In this paper, the authors explore young people's (11-18) data literacy. Data literacy is understood as the awareness of data-related rhetoric and data flows. This study forms a part of the "Exploring Data Worlds at the Public Library" research study that explores how libraries can address data literacy programming by helping teens understand, create and manage the digital traces of their data in meaningful, efficacious, and ethical ways.

Findings suggest that the 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. Data was mostly understood to mean quantified measurements, or within the presentation structure of numbers (i.e. pie charts etc). Some were able to connect data to "digital traces" and understood it as evidence. In using metaphors to explain data, participants seemed to imagine data as static, held in a single place. A few described it as a web or spread out, and some linking data to digital contexts. Teens had a broad understanding of the lifecycle of data, particularly the beginnings and ends of the cycle, but 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.

14. boyd d and Marwick AE. (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.

Age: "teenagers" (14+ but does not specific upper band) [categorised as: "teenagers"]
Privacy Type: interpersonal
Data Type: given
Method: interviews, observation (mixed-methods)
Country: US
Study Focus: behaviours, strategies, attitudes
Platform: General

This conference paper challenges the idea that teenagers reject privacy as a value, positing that they value privacy, but their definitions of privacy vary. Their practices in networked publics 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.

Authors define privacy as a social construct reflecting values and norms, with people's understandings and definitions reflecting diverse approaches and dismantling a universal notion of privacy. Teens' explanations of privacy are embedded in the realities of their lives- understand the spatial dimensions of privacy, but do not agree with a dichotomisation of privacy (public/intimate) especially when achieving physical privacy can be difficult for young people who often share spaces with family and siblings and 'home' is no longer a private space. The absence of parents is identified as a key factor in feeling as though they have privacy, underscoring that they focus more on who is present in a space rather

than its particular configurations. Access is also a key part of how privacy is understood and operationalised- boundaries to access as a form of information flow/control. Highlight the importance of control and personal agency, and their struggle to assert control especially when technology usurps or undermines their agency/control. Teens aware of and acknowledge the lack of control in relation to those who have power over them- parents, for e.g. - who violate boundaries that teens create or assert. While their engagement online is 'public', taking their images or text out of context (for an assembly on 'privacy', for e.g.) is a violation of teens' social norms or what is considered social decorum. This underscores that parents or authority figures ignore and transgress the boundaries and norms that teens assert, reinforcing the idea that teens do not have the required social cache or status for rights associated with privacy.

Networked publics- teens' engagement in these spaces take on democratic and social roles (allowing one to make sense of the world and their relationship to society) but are often restricted from entering spaces (publics) they wish to enter and can thus push to them to create their own publics (which, networked publics often are). Uses Nancy Fraser's "subaltern counterpublics" to understand practices of young people engaged in resisting and challenging adult-imposed discourse or authority (and explore their own identities and interests in relation/resistance to the norm). The social space of networked publics takes on greater significance as their interactions are less significantly influenced or controlled by adults (as often occurs in physical spaces), and these spaces take on critical value in terms of social expectations and norms. Networked publics function as communication channels, but also as the space holding their "imagined community".

Four affordances affect networked technologies (persistence, replicability, scalability, searchability) which requires contending with dynamics not usually encountered in daily life- the imagined audience for their posts/performances, the collapse and collision of social contexts, and blurring of public and private. How the social constructs of publicity and privacy are understood have been changed by social media: most interactions have been understood as 'private-by-default' and 'public-through-effort' but the opposite needs to be assumed in social media contexts. Authors assert that teens focus on what to protect rather than what they ought to disclose- this focus on exclusion is carefully studied and considered, and as a conscious choice.

The disclosure forms part of a trade-off that teens engage in- they weigh up what they might lose or gain or what the risk/reward may be. They don't consider just a 'loss' of privacy, but what they might gain from this loss- a connection or a signalling of trust. They also use the multiple communication channels afforded to them by using private dyad communication channels- text messaging or private messenger- to discuss more intimate and personal matters. Teens are also confronted by

their lack of complete control over what others share about them- sites allow tagging or @-ing in responses, for example; exacerbating the public-by-default nature of networked publics and forcing teens to consider what they wish to obscure (rather than publicise).

Teens engage in boundary management, asserting social and behavioural cues. These signs are not always followed online- either because they aren't recognised as such by adults or because they engage on their own terms, ignoring teens' agencies. Teens see privacy as embedded in context- of who is present and what is then socially appropriate given their presence and the context. Boundary management and privacy concerns collide in the prevalent 'nothing to hide' because they're not being bad model of privacy[5]- this is desire for privacy, however, is not about 'hiding' but about asserting control. Teens also segment friend groups- within services and between them- as a form of boundary management. "Social steganography"- another form of boundary management- allows teens to de/code messages for their intended audience or use language/specific references for their intended audiences.

15. 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.

Age: 9-17, 13-17 [categorised as: 8-11, 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: interviews, modular survey (mixed methods)
Country: Argentina, Philippines, Serbia, South Africa
Study Focus: digital skills, behaviours
Platform: General

The Global Kids Online project uses a child rights framework, recognising children's diverse contexts and lives while also offering a unifing approach to children's everyday online and offline experiences. The authors found that children predominantly access the Internet at home and through mobile devices. While mobile devices allow flexibility of use and enhance opportunities, it can also reduce access to support from parents and caregivers. There were clear age trends observed in all four countries: older childen were more confident in their digital skills than younger children. In particular, young children showed less competence in managing online privacy settings such as removing people from their friend's lists. A substantial minority of children in the study reported being in online contact with someone they have not met in person. Children also

[5] Solove, D. J. (2004). The digital person: Technology and privacy in the information age. New York: New York University Press

reported being bothered by internet scams, pop-up advertisements, and people sharing too much personal information online.

16. 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: 167-182.

Age: Does not specify beyond 13.6 as the average age. [categorised as: 12-15]
Privacy Type: interpersonal
Data Type: given
Method: survey
Country: USA
Study Focus: behaviour, attitudes
Platform: General

This study examines factors influencing pre-teens and early teens' private information sharing behaviour. Results suggest that their information sharing behaviours are affected by two significant factors (i) users' perceived importance of information privacy, and (ii) information privacy self-efficacy. Information privacy protection behaviour vaires by gender, and educational opportunities relating to internet privacy and computer security have a positive effect on privacy protective behaviour.

Defines information privacy as "the claim of individuals, groups, or institutions to determine of themselves when, how, and to what extent information about them is communicated to others". Uses social cognitive theory and protection motivation theory to build conceptual model for information privacy protection behaviour (i.e. behaviour influenced by gender, information privacy axiety, self-efficacy, and perceived importance- all of which influence each other too). Study findings suggest that those who have strong self-efficacy towards information privacy and have been exposed to information from external sources are more likely to practice online information privacy behaviours (i.e. not opening e-mail from unknown senders, protecting personal information). Parents' privacy concerns affected behaviour positively. Perceived importance of information privacy was critical for maintaining information privacy. Those with bad experiences online are likely to experience privacy incidents in the future.

17. 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.

Age: 0-8 [categorsied as: 0-3, 4-7, 8-11]
Privacy Type: interpersonal
Data Type: given

Method: interviews
Country: 21 countries: Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Finland, Germany, Italy, Latvia, Lithuania, Malta, Netherlands, Norway, Portugal, Romania, Russia, Slovenia, Spain, Switzerland, UK
Study Focus: behaviours, attitudes
Platform: General, mobile phones

Increasingly, very young children are showing patterns of Internet use, and most children under 2 in developed countries have a digital footprint/online presence through their parents. Study conducted across 21 countries in Europe explores how children under 8 engage with digital technologies, and parents/family members' perceptions and management of technology use.

Authors found that children's first contact with digital technologies and screens was at a very early age (below 2) often through parents' devices. Children learn to interact with digital devices by observing behaviour of adults and older children, learning through trial and error and developing their skills. Children reported using digital technology for (i) leisure and entertainment, (ii) information and learning, (iii) creation, and (iv) communication. Findings showed that a minority of children, around age 6, were social networkers; invited by their parents and generally integrated into family account. Children did not have clear understanding of privacy, or how to protect it. Parents too did not initially mention privacy as a threat, but in the follow-up interviews, some parents (in Belgium) were aware of privacy cocnerns.

18. 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: Chowdhury G, McLeod J, Gillet V, et al. (eds) *Transforming Digital Worlds. iConference 2018. Lecture Notes in Computer Science.* Springer, Cham, 442-452.

Age: 11-18 [categorised as: 8-11 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given, traces
Method: interview
Country: USA
Study Focus: attitudes, behaviours, digital skills,
Platform: SNS

This study explored teens' affective, behavioural, and cognitive states in relation to the personal data they generate on social media. Uses Ostrom's ABC model, which defines three components of attitudes as A- affect, B- behaviour, C- cognition. The ABC model explains relationship between teens and their personal data, allowing an exploration of the possible interaction between the three components.

Findings suggest that young people feel positive about their data skills, but are less certain about data privacy issues; and those with negative affective states relating to data privacy are more likely to make an effort to secure their online data. In particular, teens were confident when (i) discussing who controls their data, and (ii) discussing their skills and aptitudes in relation to data. They believed that data they created were controlled by themselves, and they displayed interst and curiousity with relation to data. Some teens showed strong negative feelings about data being tracked or recorded, feeling a loss of empowerment. Some reported ambivalent or seemingly neutral states with regard to data privacy loss. Affective states may influence behavioural strategies- those with negative affects tended to adopt behaviours to target potential threats (hiding personal info, increasingly security settings). Those who report positive affects may rely on existing routines.

19. 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.

Age: 8-12 [categorised as 8-11, 12-15]
Privacy Type: interpersonal
Data Type: given
Method: FGD
Country: UK
Study Focus: attitudes, behaviours,
Platform: SNS

This report explores the social media lives of children 8-12 in the UK (n=32) to understand the impact of social media of their wellbeing. Snapchat, Instagram, Musical.ly, and WhatsApp were the most popular social media apps, but older children had developed more of a habit; using it several times a day unlike the younger children. Social media contributes to their happiness- silly videos, for example- and allows them to be creative and play games. Children also began to see offline activities through a "shareable lens".

Parents and educators have successfully ingrained cautiousness around online risks pertaining to predators and strangers, but children were less aware of how to protect themselves from other risks affecting their mood or emotions.

20. 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, 1-68.

Age: 12-15 [categorised as: 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given

Method: participatory
Country: UK
Study Focus: behaviours, privacy strategies, attitudes
Platform: General

Child juries examined a broad range of claims and evidence, followed by discussions on fundamental digital rights. Five scenarios were performed that allowed a process of deliberation. Scenarios included:

(i) **the right to know: a scenario about the kind of personal data that's regularly tracked and stored when people go online:** young people recognised the different standards operating online with data sharing and tracking. They also shared feeling exposed and vulnerable as a result of this data sharing. Argued that companies should not be able to store data about them, while some suggested that informed consent needed to be a cornerstone of any data storage; leading to questions about T&Cs. Jurors recognised that T&Cs were complicated and long, and many did not read through them but agreed to what they contain. Jurors proposed concerete recommendations for how data is collected and stored, and its relationship to T&Cs.

(ii) **the right to delete: a scenario about online content that children and young people want to delete because it might be embarrassing or inconvenient:** The scenario resonated with jurors, but were split between people who believe that one ought to take personal responsbility for content they share; and those that felt they ought to be protected against leaving permanent traces of their immature selves. They identified the porous nature of the Internet, and how even if content is shared on a specific platform it can be circulated beyond that space. Lack of technical knowledge about the architecture of the Internet contrained recommendations. Also reflected jurors' lack of knowledge about data generated by or about them.

Findings suggest that young people believe that the online-offline dichotomy must be transcended with the same rights and responsibilities in online spaces as in offline ones. They wanted regulations to ensure safe and happier online experiences for young people, including the right to edit or delete content; and opportunities to repair their mistakes. Participating in the juries positively affected their efficacy, engendered a determination to participate in and shape how digital technology services are run.

Juries developed several recommendations about data use, data tracking, self-tracking where data travels, and demands for broader curriculum that improves internet literacy.

21. 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.

Age: 11-19, mean age is 14.8 [categorised as: 8-11 12-15 16-19]
Privacy Type: institutional
Data Type: given
Method: FGD, questionnaire
Country: USA
Study Focus: behaviours
Platform: mobile phones, laptops and tablets, SNS

Study examines technology in academic contexts, and privacy-relevant youth practices. Respondents identified restrictions to internet use in schools with blocking and filtering measures in place which often block social media platforms. The filtering mechanism can result in blocking platforms relevant for academic research. While the restrictions caused respondents frustration and annoyance, they also knew about workarounds or were able to ask friends to help circumvent them. They also sometimes brought their own devices with Internet access.

Respondents were also aware that school officials attempted to monitor their behaviour online. They identified screen-surveillance software (which allows supervising adult immediate access to the screen with a subtle notification to student), and were suspicious of school platforms that allowed communication in case it could be intercepted. Some narrated how school officials- teachers, adminitrators- were able to access their social media behaiour; making them uncomfortable.

22. Culver SH 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.

Age: 14-25 [categorised as 12-15. 16-19, and additional category of 20-25]
Privacy Type: institutional, interpersonal
Data Type: given
Method: survey (quasi experimental)
Country: 100 + countries (coded as global, 100 countries unesco)
Study Focus: media literacy,
Platform: General

This report sees media and information literacy (MIL) as an understanding of how media and information are created, analysed, distributed, applied, and used; as well as monestised; requiring critical skills. Privacy competencies are, thus, a key part of MIL competencies; including the ability to demand one's right to privacy, act wisely about information sharing, and how to secure one's information.

Key findings: majority of respondents (74% strongly agree, 23% agree) indicated that privacy is important to them.

Institutional privacy: 60% of survey respondents disagreed that governments have the right to know all personal information about them, but shifted when on questions relating to security and safety. 38% of those surveyed strongly agreed/agreed that governments have the right to know this information if it will keep them safe online. 55% place a higher priority on their security than their privacy, 31% responded with 'neutral' – authors interpreted this to mean that they were unsure of which they valued more or that they valued them equally. 50% strongly agreed/agreed that the Internet should be free from governments' and big businesses' control.

Respondenst did not receive much MiL training relating to privacy- 56% said it was addressed for one hour or less over an entire course.

Draws parallels between Cannataci, Zhoa et al (2016) analysis of three pillars of privacy, transparency, and freedom of expression; and likened it to rights to privacy, freedoms of expressions and of information. Authors highlight the constantly shifting interplay between the three pillars and these rights, where the values surrounding them are constantly in flux.

Authors suggest that (i) an awareness of the commodification and monetisation of personal profiles; and (ii) an understanding of the duties of institutions in cyberspace are key compotents of privacy competencies and are valuable for construction of privacy.

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

Age: 10-14 [categorised as 8-11, 12-15]
Privacy Type: interpersonal
Data Type: given
Method: in-depth interviews
Country: USA
Study Focus: attitudes, privacy strategies, support
Platform: SNS

This empirical study explores middle school students' ("tweens" 10-14 years old, n=42) online privacy practices. It investigates their online activities including texting, use of mobile phones, IMs, playing games, and SNS (Facebook and Myspace). Participants reported that they were under-age users of SNS.

Tweens' privacy definitions tended to be interpersonal understandings of privacy, focused on maintaining control over their information and protecting it from unwanted audiences. While unwanted audiences often

meant strangers, and a fear of strangers was evident; they were more likely to discuss wanting privacy from a known other such as friends and family members. Tweens mentioned institutions such as police or government less frequently. One participant mentioned advertisers ("spammers"). In terms of privacy management online, participants relied on withholding or proactive strategies.

Withholding strategies: Nearly all participants discussed withholding content from online spaces, first considering the (in)appropriateness of the information they post, such as private or embarrassing information. *Proactive strategies*: Participants discussed adjusting privacy settings, embedding false information, untagging/deleting photos, or using multiple accounts online. *Absent strategies*: Some participants reported being unware of privacy options.

The participants said they turn to close relations for advice on managing their own/others online privacy; and check before posting photos. 3 teens created explicit privacy guidelines with friends and family. They also discuss 'reflection' as a tool- to think before you post, as once posted it 'stays'. Participants made a conscious choice to accept the default privacy settings on SNS and other platforms based on the belief that the site designers and developers already considered privacy issues, and built adequate privacy protections into the site's architecture.
Their digital literacy lessons on privacy are focused on strangers/stranger danger, overlooking the full range of youth's online privacy concerns. The authors did not find evidence of social steganography- suggesting that this may be because that while tweens do use forms of steganography they don't consider it in terms of online privacy. It may also have to do with developmental maturity and their understanding of the social complexity online, given this particular age group.

24. De Souza Z and Dick GN. (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: 255-261.

Age: 12-18 [categorised as: 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: questionnaire, FGDs
Country: Australia
Study Focus: behaviours, attitudes
Platform: SNS (MySpace)

Study compares the level of information disclosed by young (12-18, n=263) MySpace users with the value attributed to privacy concerns, in an attempt to identify a correlation between the concern attributed to privacy and their actual behaviour. Authors draw on literature detailing

reasons for information disclosure: signalling, peer pressure, displays of connection, trust, myopic view of privacy risk, design interface, relaxed attitudes to privacy; which forms their research model framework.

Authors administered a questionnaire to understand what information young people share on MySpace, and used some participants' MySpace websites to confirm self-reporting accuracy. The auestionnaire also measured viewpoints on the drivers of information disclosure, and the value of privacy to the user. They also conducted 2 FGDs- one with parents, and one with children. The children's FGD asked for feedback and comments on their analysis.

Findings suggest that information disclosure was driven by three factors: peer pressure, design interface, and signalling. Peer pressure may influence a user to share information because their friends have, and the interactivity of friends sharing information may be increased if they all have information rich profiles. Design interface- "I put that information because there was a place/box to enter it"- drives the user to to fill in a number of fields collecting personal information. Users are more likely to fill it as they mistakenly believe it is mandatory or because its template and page setup appears to influence disclosure. Signalling suggests that the more the user desires to portray themselves in a certain light, the more likely they are to disclose information; and relates significantly to their identity production.

Trust, relaxed privacy attitudes, and myopic evaluation of privacy risks did not play a role in determining the level of information disclosure. The lack of effect of trust may be because users may not trust the platform but still disclose information due to the other drivers. Analysis also indicates that privacy may not play a role in an individual's decisions when interacting with applications at a certain point in time. Users who attribute a higher value to their personal privacy were less likely to disclose as much information on their profiles.

25. Dennen VP, Rutledge SA, Bagdy LM, 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.

Age: 10th and 12th grade students [categorised as: 16-19]
Privacy Type: interpersonal
Data Type: given
Method: participatory, observation, survey (mixed-methods)
Country: USA
Study Focus: behaviours, privacy strategies
Platform: SNS

This study explores high school students' (10th and 12th grade, K-12 charter school) in-school and out-of-school communities in a social media context. Students (n=48) attended a 3-day unit on social media networks and context collapse where they explained their communities, social media networks, and discussed social media use in and out of school. Findings show that students experience context collapse, but rather than seeing it as a negative occurrence they expect it as a part of networked digital environments. They are adept at managing context collapse, use different means to communicate online with different groups; maintain separate technological lines, and using more private spaces for private exchanges than those afforded by social networking tools.
Student communities included personal communities (groups student belong to outside school- church groups, sports groups etc.), school community (school-based clubs etc., including friendship groups). There were differences in which tools were used to connect with different communities – Instagram or GroupMe for group activities like team sports to enable a shared online space. While other tools such as a YouTube or Twitter were used, they were used more passively. Students were intentional about the tools they used- Snapchat was likely to be used with people they knew in real life, unlike their Twitter use.
Students were highly attuned to who they connected with and how, what they shared online, how to use different tools and multiple accounts for different purposes. They were adept at managing context collapse, readily acknowledging and recognising it in their communities.

26. Dey R, Ding Y and Ross KW. (2013) Profiling high-school students with Facebook: how online privacy laws can actually increase minors' risk. *Proceedings of the 2013 conference on Internet measurement conference.* Barcelona, Spain: ACM, 405-416.

Age: "secondary school" – 14-18 [categorised as "teenagers"]
Privacy Type: commercial
Data Type: profile
Method: Experimental
Country: USA
Study Focus: interface/design/settings
Platform: SNS

The authors demonstrate the feasibility of profiling secondary school students using Facebook and discuss the associated privacy threats. Applying the profiling methodology to a small private high school and two relatively large public high schools located in different regions in the USA, the research team was able to identify between 79% and 85% of all students in the respective schools with false-positive rates of between 22% and 32%. For most of the students, they discovered 'private' information minimally including current city and school, graduation year, inferred year of birth, and list of school friends. For about half of the students they were also able to find varying amounts of additional

information, such as shared photos and wall postings. Significantly more information is often directly available (depending on privacy settings) for minors registered as adults. The consequential threats relate to: brokers selling the data to other agents (advertisers, further education recruiters, and employment agencies), fuel a large-scale and highly personalised spear-phishing attacks, exposure to perpetrators of child sexual abuse and violence.

27. Emanuel L and Fraser DS. (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.

Age: 13-18
Privacy Type: interpersonal
Data Type: given, traces
Method: participatory, survey
Country: UK
Study Focus: attitudes and values
Platform: General

This study (which is also part of a larger project- SuperIdentity) explores teenagers (n=31)' attitudes, values and concerns relating to privacy and identity information in online and offline spaces.

Authors emphasise that identity has multi-faceted- not only physical and personality attributes and behaviour patterns. All identity facts also exist and are represented in the digital world, along with unique digital identity attributes such as e-mail or IP address. Teenagers move fluidly between online and offline interactions, and their understandings and values relating to privacy must take this into consideration as personal information is increasingly collected and collated across environments.

Teenagers use multiple interactive platforms to fulfil different facets of information sharing and interactions with people mirroring the choices they have to share information face-to-face. The participants perceived different networks and online platforms as offering varying levels of privacy based on the target audience for participants' information (for e.g.: YouTube as public, Skype as private). Participants shared that they felt information posted online was more permanent, reflecting that they had little to moderate control after it has been posted online. Unintended sharing of personal information by 'friends' in online settings was perceived to be the biggest threat. The diverse SNS used were not seen to offer privacy protection with overlapping friend networks and services that link together different SNS accounts; making compartmentalisation difficult. Blurry digital and physical divides due to the ubiquitousness of technology, as communication via tablets and smartphones in physical environments was parallel with private messaging in online platforms. Concerns around this bridging were around connecting physical-base

information (phone number for e.g.) to cyber-persona (e-mail id, for e.g.), but the same level of concern for the reverse was not present.

Avatar design workshop (where participants design an avatar, fill out form about physical identification/features, and then a peer fills in a form based on the avatar): participants tended to try out different looks but majority settled on features similar to their own. Some suggest it is so their friends can recognise them, but also suggest that under certain circumstances they would trust the accuracy of the avatar as reflective of its creator. They were sceptical that an avatar would provide valuable identity information to unfamiliar or unknown individuals. Admitted using other identifiers such as favourite colours or background pictures related to their interests but did not view it as linked back to them as a person, feeling that information regarding their interests was not particularly unique and couldn't be used to identify them in offline spaces.

Different online spaces were used as a means for controlling the flow of information, indicating some understanding of different audiences consuming information and allowing them to compartmentalise their identity information. However, this diversity also creates a rich identity footprint that they were not always aware of.

28. 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: 153-162.

Age: 12-17 [categorised as 12-15. 16-19]
Privacy Type: interpersonal, commercial
Data Type: given, traces
Method: secondary analysis
Country: USA
Study Focus: behaviours, strategies,
Platform: SNS (facebook)

This study uses Pew Internet's Teens and Privacy Management survey to explore socialisation agents of teens' online privacy concern and the relationship between teens' level of concern and their privacy behaviours. Analysis shows SNS use and parents' privacy concerns as motivating factors in teens' increased privacy concern, driving adoption of privacy-setting strategies.

Uses Westin's (1967) conceptualisation of privacy to frame the study, including the shift in public trust in information collection activities by government and other agencies; pushng privacy to a first level social issue in the US. Complements this with Lessing's (1998) understanding of privacy as what is left over after removing what can be monitored and is

searchable from one's life; given the ability to mine data and the availability of large scale data sets such as Facebook allowing advertisers and third parties easy access to observe, track, and monitor behaviours. As COPPA doesn't cover marketers' collecting voluntarily shared information on SNS, teens are likely to be unaware of the implications and is a cause for concern. Parents' roles as socialisation agents is emphasised as they shape young peoples' consumer norms and marketplace knowledge.

Results showed that parents were concerned about markerters collecting children's data, and there is a positive relationship between their level of privacy concern and that of their children. Results also reflect on theoretical underpinnings as parents' concerns drive teens to adopt more privacy-setting strategies. SNS usage was a another socialisation agent that increases teen's privacy concerns about marketers, as increased media use is related to development of consumer knowledge and scepticism. Female and older teens tended to spend more time on SNS. Teens whose parents/guardians 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 teens' level of privacy concern and their privacy-setting strategies- they more likely to set their profile to private or partially private if they were concerned with privacy.

29. 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, USA: International Communication Association, 1-27.

Age: 13-17 [categorised as 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: interviews
Country: USA
Study Focus: attitudes, behaviours, privacy
Platform: General

Study explores how young people (13-17) negotiate online friendships and online privacy concerns. Authors suggest that they do not negotiate the two concerns separately but instead situate their understanding of online privacy within their conceptions of online friendship, showing that ideas of privacy/personal security are less about the particular technology or platform, but rather the type of relationship that it supports or enables. Analysis indicates that the understandings of privacy and security are applied to ecosystems of technology used to support two primary types of mediated friendships: affective and instrumental, rather than individual technologies alone. Instrumental friendships are based around common interests or task-oriented. Affective friendships reflect a deep appreciation

for the other and generally seen as irreplaceable; also friendship-driven or interest-driven.

Teens participating in the study were keenly aware of online risks, expressing a strong desire to keep their mediated communications safe and private. Explained conscious and thoughtful decision-making processes about sharing personal information, largely based on the relationship they were attempting to support or build. Suggest that rather than concluding that the privacy paradox reflects lack of knowledge or that teens prioritise socialisation over privacy; teens do not treat friendship (i.e. their interactions online) and privacy separately but in light of each other; and in a technological ecosystem to support these relationships. In affective friendships, technology is less salient and may be used interchangeably, designated the same security and privacy levels as in face to face communications. This may mean they worry less about the risks of disclosing personal/private information when using them (not necessarily that the risks are, in fact, lower). Instrumental friendships, however, sees technology take on an extremely salient role, often forming the basis of the frienship- clearly using a variety of strategies to keep 'online' and 'offline' worlds separate.

30. Gelman SA, Martinez M, Davidson NS, et al. (2017) Developing digital privacy: Children's moral judgements concerning mobile GPS devices. *Child Development* 89: 17-26.

Age: 4-10 [categorised as 4-7, 8-11]
Privacy Type: interpersonal,
Data Type: traces
Method: experimental
Country: USA
Study Focus: interface, attitudes, literacy
Platform: GPS devices

Mobile tracking devices offer valuable affordances but can compromise privacy and anonymity. By age 3, children have firm understandings of property rights- that nonowners may not use others' objects without permission. By 6-8, children extend ownership rights to non-physical items. This study conducted three experiments to understand children's opinions around location tracking through their/another's possessions through a mobile GPS device.

Each experiment demonstrated how GPS mobile devices functioned and asked to judge acceptability of someone else tracking their possessions or their tracking someone else's. Experiment 1 examined reactions to tracking a device (that is placed on an object by someone) via a computer. Experiment 2 examined reactions to placing a device on an object but not tracking it. Experiment 3 examined reactions to someone tracking the device when the owner has placed it on an object. The experiments allows differentiation of perceived implcations of tracking

from perceiving implications of one's personal space being violated by physical contact.

Experiment found that youngest children (4-5) did not appear to evaluate use of mobile GPS device in terms of ownership rights as it seems that tracking and attendant privacy issues are not a concern at this age. At 6-7 years of age, this sensitivity begins to emerge, as they (like adults) judged it to be relatively more permissable for owners than non-owners to track their own possessions. By 5 years, they saw placing an object to track someone else's possessions to be less acceptable than tracking their own, and by 6-7 years of age invoked moral considerations to explain their beliefs. Yet, children were more accepting of this behaviour than adults, focusing on the benefits of object tracking. Authors suggest that one reason why intuitions differ so dramatically may be because young people are relatively trusting of others and do not spontaneously consider the negative consequences of revealing personal information. Adults' responses tended to focus on morality, privacy, and ownership principles rather than negative outcomes themselves. Authors speculate that developmental changes in independence may heighten the value placed on (digital) privacy. More experience with electronic devices may result in greater awareness of the consequences of tracking.

31. Ghosh AK, 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.

Age: 8-19 [categorised 8-11, 12-15, and 16-19]
Privacy Type: interpersonal
Data Type: given
Method: Content analysis
Country: unclear (USA-based, but potentially international- marked as 'global')
Study Focus: attitudes, behaviours, interface
Platform: General

The existing privacy theories gravitate towards the notions of information disclosures and visibility – networked privacy (Marwick and boyd, 2014)[6] refers to disclosure within friendship circles on social media platforms; Nissenbaum's (2004)[7] theory of privacy as contextual integrity refers to the negotiation of privacy norms and cultures; and the communication privacy management theory (Petronio, 2002)[8] frames privacy as a boundary negotiation process. While all these approaches assume some level of control over disclosure decisions, they fail to address that in

[6] Alice E Marwick and danah boyd. 2014. Networked privacy: How teenagers negotiate context in social media. New Media & Society 16, 7: 1051–1067
[7] Helen Nissenbaum. 2004. Privacy as Contextual Integrity.Washington Law Review 79, 119
[8] Sandra Sporbert Petronio. 2002. Boundaries of Privacy: Dialects of Disclosure. SUNY Press.

relation to children, decisions are often limited (for example, by parental technical mediation or lack of engagement of children in product design). Based on thematic content analysis of 736 reviews of 37 mobile online safety apps from Google Play that were publicly posted and written by children (aged 8-19), the study explores children's perceptions of parental control apps. The findings suggest that a majority of the teen reviews were low-rated (79%, N=581) as the children found the apps overly restrictive and obstructing everyday tasks such as doing homework or limiting the amount of time they can spend using the device. Teens also felt that the apps were invasive to their privacy (resembled parental stalking and felt disrespectful) and did not facilitate communication or trust between parents and children. There were positive comments which reflected children's appreciation of helping control undesirable practices (related to time spent, concentration, pornography) and helped them feel safer.

32. 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: 81-87.

Age: 12-18 (mean age:15.35) [categorised as 12-15, 16-19]
Privacy Type: commercial
Data Type: given
Method: survey
Country: Belgium
Study Focus: privacy concerns, attitudes?
Platform: SNS

This study uses a global theoretical framework to predict adolescents' personal information disclosure in order to access incentives (free products, discounts) offered by commercial platforms and websites. Draws on literature that suggests teenagers have more difficult than adults in resisting temptation where incentives are present, and young adolescents are less concerned about potential risks of information disclosure. Uses Westin's concept of information privacy, and suggests that in an online content it also refers to individual users' decisions about whether to disclose private information when requested by a commercial entity.

This study tests the applicability of 'theory of planned behaviour' to disclosure of information by teenagers in response to incentivised online data requests. Findings suggest that subjective norms are the most important predictor of teenagers' intentions to disclose. Social pressures can thus outweigh individual attitudes and subjective evaluations of information privacy. This impact of social pressure is linked to their social development and learning where their exposure to others' opinions can exert pressure. Authors found a direct positive relationship between

perceived behaviour control and disclosure, suggesting that information disclosure is informed- in part- by availability of opportunity.

33. Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (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. doi:10.1145/3134699

Age: 5-11 [categorised as 4-7, 8-11]
Privacy Type: interpersonal
Data Type: given
Method: interviews
Country: USA
Study Focus: media literacy, supporta and guidance, behaviour
Platform: General

Qualitative study (semi structured interviews, and hypothetical scenarios) with 18 (23 parents, 26 children) US families with children ages 5-11 (median =8) to explore how children perceive and address privacy online. Uses some developmental theory- 'theory of mind', and ability to grasp 'secrecy' that is necessary for information management abilities.

Uses contextual integrity framework, findings suggest that while children recognise certain privacy and security components, younger children (5-7) have knowledge gaps. While children develop their own strategies, they tended to rely on parents for guidance; who primarily used passive strategies to mediate use or deferred it to the 'future'. Children's distinction of online/offline behaviours are blurred, affecting viewpoints on privacy and security.

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

Age: 12-15 [categorised as 12-15]
Privacy Type: interpersonal
Data Type: given
Method: interview
Country: UK
Study Focus: attitudes/beliefs, strategies
Platform: General

A qualitative study of 16 UK children aged 13-16 years 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 own understanding of friendship and intimacy on privacy norms and behaviours.

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

Age: 11-16 [categorised as 8-11, 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: Survey
Country: Ireland
Study Focus: Attitudes and beliefs, behaviours
Platform: Social media

The article is based on a survey with 474 Irish teenagers aged 11-16 years and explores some of the risks they face on social media (Facebook, Bebo, Twitter), including bullying, inappropriate contact, overuse, addiction and invasion of privacy. Privacy invasion is understood as unintended access to personal information. The authors conclude that the teenagers 'are not hesitant to share specific personal information online, thereby exposing their private lives and increasing the potential for unintended invasion of their privacy' (Machold et al., 2012: 152) but no further details are provided.

36. 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

Age: 12-17 [categorised as 12-15, 16-19]
Privacy Type: interpersonal, commercial
Data Type: given, data traces
Method: Survey
Country: USA
Study Focus: Behaviour, privacy strategies
Platform: General but includes SNS

A survey of 802 teens show that they share online more personal information about themselves than in the past including posting photos of themselves (91% do this), their school name (71%), the city where they live (71%), email address (53%), and mobile phone number (20%). Teens also share their real name (92%), their interests (films, books, music they like, 84%), birthday (82%), relationship status (62%) and videos of themselves (24%). This is explained by both the evolution of the platforms which are designed to encourage sharing, as well as by the changing norms around sharing online and socialising. 16% of teenagers automatically include location in their posts and 33% of teenagers are friends with people they do not know (more so for older teens). Older teens socialise online with a wider variety of people including teachers or

friends from different schools. The majority of social media accounts are private – 64% of Twitter accounts, 60% of Facebook profiles, with girls being substantially more likely to have a private account than boys (e.g. 70% vs 50% of Facebook profiles). Most teens are confident in managing their social media privacy settings (only 9% find it somewhat or very difficult) but younger children struggle more - 41% of Facebook users aged 12-13 say it is "not difficult at all" to manage their privacy controls, compared with 61% of the children aged 14-17. In addition, teens take other measures to protect their online privacy or reputation – deleting or editing something that they posted (59%), deleting comments from others (53%), removing tags (45%), deleting or deactivating an entire profile or account (31%), deleting (74%) or blocking (58%) people, posting fake information (26%). Still, 19% say that they have posted something online (updates, comments, photos, or videos) that they later regretted and 40% are ("very" or "somewhat") concerned that third parties (advertisers or businesses) might access some of the information they share. Younger teens are more concerned than older - 17% of the 12-13-year olds are 'very concerned' vs. 6% of the 14-17-year olds. The teens who are more concerned are also more engaged in strategies for online privacy management as are those who are more active users and have larger networks and share more content. More than half of teens (57%) say they have decided not to post something online because they were concerned how it might affect them in the future with those using social media being more likely to report this.

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

Age: 12-18 [categorised as 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: qualitative
Country: India
Study Focus: Behaviour (practices)
Platform: SNS

The study explores the practices of and motivations behind photo tagging (perceived usefulness, positive and negative aspects, tagging preferences) of Indian youth. The method used is described as 'qualitative essay-based questionnaire' which is unclear. The study found that boys were more engaged in photo tagging than girls and saw this as a way of getting more likes, comments, and attention – a symbol of higher status in their peer group. They carefully considered the photos and people they wanted to tag and how frequently to do it. Girls did not see tagging as a form of social status and preferred to be tagged by close friends and family only. They were also less concerned about appearances than boys. These differences are explained with 'privacy concerns and parental influence' (page 12) as many girls saw tagging as unnecessary or as an

intrusion of personal space and privacy. The girls were also less knowledgeable about online privacy settings and more worried about misuse of personal photos which made them less comfortable with photo tagging.

38. Martin F, Wang C, Petty T, et al. (2018) Middle School Students' Social Media Use. *Educational Technology & Society* 21: 213-24

Age: 12-16 [categorised as 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: survey
Country: USA
Study Focus: Behaviour (practices)
Platform: SNS

Based on a survey with 593 students from two schools in Southeast USA, the study explores the participants' use of social media and their opinions towards online safety. The findings suggest that young people try to protect their personal information mainly from adults (parents and teachers) while their awareness and abilities to protect their privacy and personal information online from others is more limited. The study also found that girls are more likely to contact strangers online, to have an SN profile earlier on, and to check their social media for updates much more often than boys.

39. 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, Colorado, USA: ACM, 5197-207

Age: 6-10 [categorised as 4-7, 8-11]
Privacy Type: commercial
Data Type: given, data traces
Method: interviews
Country: USA
Study Focus: media litaracy, behaviours
Platform: Connected toys

The rising popularity of internet-connected toys are posing new privacy threats related to children's data. The study involved semi-structured interviews with nine parent-child pairs and an observation of the child playing with internet-connected toys Hello Barbie and CogniToys Dino, focusing on the exploration of parents' and children's perceptions of privacy. The study found that children got quickly bored with the limited responses of the toys. While 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, children were often unaware that the toy recorded what was being said to it. Not all children knew that their parents could listen to the recording and even those who did seem to understand that were still willing to tell the dolls a secret. Parents doubted that they would have the time to listen to the recordings and check what data the company has on their child, but some appreciated the opportunity the toy offered them to monitor their child. The parents also wanted to have some parental control over what the toy can say to the child and when it records.

40. 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

Age: 10-17 [categorised as 8-11, 12-15, 16-19]
Privacy Type: commercial
Data Type: given, data traces
Method: FGD
Country: Canada
Study Focus: attitudes, media understanding
Platform: General

Drawing of focus groups with 54 children aged 10-17, the authors discuss the participants' interpretation of privacy policies on a few favourite children's sites (discussed fragments from the policy of neopets.com, doyoulookgood.com and addictinggames.com). The study found that most participants reveal personal information on the Internet as an exchange to access (to games, social networking sites, contests, or prize draws). Privacy is not very high on children's agenda and they tend to click through the policies to get to what they want. Most children did not read privacy policies as they found them too long, boring and difficult to understand: 'In reading the policies, they struggled with complicated words, convoluted sentences, confusing structure, and misleading organizational signals' (Micheti et al., 2010: 133). The children also struggled with the poor design and inadequate structure of the privacy policies. The authors conclude with a number of recommendations for privacy policy development and design.

41. 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

Age: 10-11 [categorised as 8-11]
Privacy Type: commercial
Data Type: data given
Method: experimental
Country: USA

Study Focus: behavioural
Platform: General

There has been a rise in the commercial exposure of children related to the intensified use of social networking sites and their commercial links, hence the study looks at the different safeguards that can prevent preteens from accessing unsuitable online content. A sample of 112 web sites that were identified as oriented toward children was analysed for the type of safeguards it contains. Three types of child-protection safeguards were identified: 1) *Warning safeguards* – notifying of inappropriate content or stating that the services are suitable for children over a certain age; 2) *Threat safeguards* – informing children that their registration can be reported (to parents, teachers, regulatory agencies); 3) *Barrier safeguards* - requiring parental approval (via e-mail, phone, credit card). The study found that 30% had no safeguards at all; 23% had only warning safeguards; 9% had warning and threat safeguards; and 37% had warning, threat, and barrier safeguards. A sample of 375 10- and 11-year-old children was presented with different scenarios of using a new website where the three different types of safeguards were tested. The study found that the presence of a combination of a warning and threat safeguards resulted in lower information disclosure levels while only a warning resulted in higher disclosure. Children whose parents were more actively involved in parental mediation tended to disclose less.

42. 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

Age: 14-19 [categorised as 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: interviews
Country: Germany
Study Focus: behaviours, media literacy/understanding
Platform: SNS

The paper investigates the extent to which children know what type of profile information they disclose on Facebook and to whomm, using a metacognitive accuracy model and a sample of 45 secondary school students. Most often the actual content was set to public (46%) or friends (35%), and less often to only myself (12%), friends of friends (5%), or custom (2%). The findings suggest that the students knew rather well in which categories they have disclosed information about themselves but were less sure to whom as they often struggled to name the privacy setting of their disclosed contents. The majority reported that they had changed their profile privacy so that only friends can see the content but were not aware that different types of information need to be set separately. When they were wrong they were also both

overestimating and underestimting how private their profile content was, hence there was no bias. They were overestimating the privacy of information such as favourite music and their school but underestimating the privacy of their email address or birthday. Their confusion about the audiences was explained also with the complexity of the interface.

43. Moscardelli, D. M., & 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), 232-252.

Age: 13-19 [categorised as 12-15, 16-19]
Privacy Type: interpersonal, commercial
Data Type: given, data traces
Method: survey
Country: USA
Study Focus: behaviour, beliefs
Platform: general

Children not only use the internet more heavily but they also spend more of their own money online in a context where companies have a wider arsenal of tools to collect information about their customers across platforms and match internet behaviour to personal data. Having control over one's personal data is becoming increasingly difficult – 'personal information is bought and sold like other commodities' (Moscardelli and Divine, 2007: 234). The study looks at the factors (sociocultural characteristics and sociaisation agents) associated with the development of privacy concerns and whether such concern is linked to protective behaviour amongst children. The predictor variables include sex, age, and household size (sociostructural characteristics) and socio-oriented and concept-oriented family communication style, informative and normative peer influence, do they have an e-mail address, and how often are they online (socialisation agents). Concern for privacy was measured using a 14 items 7-point scale originally developed by Sheehan and Hoy (1999), which asks respondents to rate their level of concern with various Internet usage scenarios. The study involved a survey with 1, 626 participants aged 13-19.

The results of the study indicate that the concern for privacy was posiotively associated with the amount of time spent online, the extent of concept-oriented family communication style (more inclusive of children's views), and the informative peer influence (using friends as sources of infiormation rather than tryiong to copy them). Hence, it could be argued that communication with
teens rather than rule-setting is more efficient in creating privacy awareness. The study also found that girls and children who have emails are more concerns about privacy. In turn, higher privacy concern was associated with requesting removal from e-mail lists, reporting unsolicited

e-mails or responding negatively to them, and providing inaccurate personal information.

44. Moser C, Chen T and Schoenebeck SY. (2017) Parents' and children's preferences about parents sharing about children on social media. *Human Factors in Computing Systems*: 5221-25

Age: 10-17 [categorised as 8-11, 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: Survey
Country: USA
Study Focus: attitudes, behaviours, decision-making.
Platform: General

Online survey with 331 parent- child (children aged 10-17) pairs (US) to examine preferences about what people share about children on social media. Uses communication privacy management theory- tensions arise when people don't coordinate disclosure of personal information.

Children prefer parents share positive content about them, as well as reflecting a positive family life/relationship. Content reflecting negatively on child's self-preservation, content perceived as 'embarrassing', unflattering, or overtly revealing was reported as less permissible. Photography- for positive and negative content- was a common theme.

Parents and children show similar perceptions about how often or how much information parents share about children, but disagree on the permission-seeking process. Children believe that parents need to ask permission more than their parents think they should. Parents also believe they should ask more permission more often than they do, and this was especially marked in younger parents.

Using this data, suggest design opportunities to manage family sharing on social media: 'okay to post' recommendations can build trust with children by only posting content deemed so by them, permission-seeking (explicit tagging of child by parents, that requires their approval – does not discuss age implications), learning preferences (permission-seeking mechanism allowing SNS to learn and adapt to preferences over time. Suggests an engine could collect labelled content – embarrassing etc- to understand evolving preferences. Does not engage with privacy issues in this regard), directing tone (scan posts for positive/negative text or expressions with prompt to check if really wish to share- again, does not engage with privacy-related risks associated with this)

45. Mullen, C., & 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*, 165-172. doi: 10.1016/j.chb.2016.02.026

Age: average age 15.55
Privacy Type: interpersonal
Data Type: given
Method: survey
Country: Ireland
Study Focus: behaviours, attitudes
Platform: SNS

The study draws on Communications Privacy Management (CPM) Theory (developed by Petronio, 2002) which suggests that people think they own their personal information like a possession but experience a tension between the need to control it and the need to share it. Disclosure of information is influenced by culture, the context and one's gender and once shared, the information becomes co-owned with others.

Of the 262 children participating in the study, just over 50% had received a friend from a parent and 70% of these had accepted. 89% had a Facebook account and 84% had accounts with between 3 to 7 different social networks, including Snapchat, Instagram and WhatsApp and only 4% of children had a public profile. The study found that girls were more engaged in privacy protective strategies but these did not predict online friendship with parents as girls were more likely to be online friends with their parents. Overall, children who had a better relationship with their parents were more likely to be friends with them online and children did not see befriending parents online as a threat (but those who disapproved it were less likely to be friends with parents). Peer influence affected attitude to friendship with parents but not the actual friendship status. The study also found that children used multiple privacy strategies including considering how much information to share, bearing in mind who they are friends with, as well as using more private channels (such as messages) for more personal information.

46. Murumaa-Mengel M. (2015) Drawing the Threat: A Study on Perceptions of the Online Pervert among Estonian High School Students. *Young,* 23: 1-18.

Age: 17–20 [categorised as 16-19]
Privacy Type: interpersonal
Data Type: data given
Method: interviews
Country: Estonia
Study Focus: attitudes and beliefs
Platform: SNS

The article explores how young people perceive the characteristics of people who engage in online sexual solicitation of children and found that such people are often seen as 'the other' and being very different. In relation to privacy, it is argued that when creating their social media presence, young people are concerned more about the present and social relationships, than what will happen in the future and develop detailed strategies for managing their audiences. At the same time they are not engage very much in privacy protection – 28% do not use any privacy settings when on social media and 50% had contacted people they do not know.

47. Ofcom. (2017). *Children and Parents: Media Use and Attitudes Report.* Retrieved from London: https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

Age: 3-11 [categorised as 1-3, 4-7, 8-11]
Privacy Type: interpersonal, commercial
Data Type: given
Method: Survey
Country: UK
Study Focus: media literacy, attitudes, strategies
Platform: General

The report examines children's (age 5-11, + media access of ages 3-4) media literacy, and parents' views of children's media use and their efforts to monitor/limit use. Online survey data analysed. Children are adopting social media sites, but report pressure to 'look popular', and parents are not always aware of minimum age requirements. Children also find it difficult to identify advertisements online- which have evolved to form a more complex advertising and marketing environment. Report knowledge of personalised online advertising and brand ambassador advertising (via vloggers etc) but are not always able to identify this in practice especially when it is designed to work similarly to other social media content. Also report understanding advertising revenue through sponsored ads but are unable to identify it accurately (even when the word 'ad' appears). Believe Google play an authenticating role, believing search results can be 'trusted' as a result. Report negative experiences but have developed strategies to report or tackle online experiences.

48. Ogur B, Yilmaz RM and Göktas Y. (2017) An examination of secondary school students' habits of using internet. *Pegem Egitim Ve Ogretim Dergisi,* 7: 421-452.

Age: 10-13 [categorised as 8-11, 12-15]
Privacy Type: interpersonal
Data Type: data given
Method: survey
Country: Turkey

Study Focus: behaviour
Platform: general

The study explores children's online practices using a survey and a sample of a 442 children in years 5 to 8. The findings suggest that 40% of children know how to change their privecy settings on social networking sites but 29% say that they don't use privacy settings even though they know how to. Young people share various information oonline – 58% share their name with everyone, 57% the city they live in, 45% had shared a photo of their face, 45% their school, 28% share their location online, 25% their birthday, 20% their relationship status, 12% share their address and 10% share their phone number.

49. Öncü S. (2016) Facebook habits among adolescents: Impact of perceived social support and tablet computers. *Information Development,* 32: 1457-1470.

Age: 10-14 [categorised as 8-11, 12-15]
Privacy Type: interpersonal
Data Type: data given
Method: survey
Country: Turkey
Study Focus: behaviours
Platform: SNS

Based on a survey with 4,261 Turkish students from middle and high schools, the research explores the sharing practices of young people, looking at importance of demographics and social support. The study found that children from larger cities, boys and older childrn were more likely to have over 100 contacts on Facebook. Children who thought they could rely on their family for support when needed were less likely to have many friends, while those who relied more on support from friends and significant others were more likely to have more contacts online. Again girls and younger children were less likely to accept requests from unknown people as did those who relied on family more.

50. 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.

Age: 13-16 [categorised as 12-15, 16-19]
Privacy Type: interpersonal
Data Type: data given
Method: mixed method (ethnography, interviews, survey)
Country: Finland
Study Focus: behaviours
Platform: blogs, vlogs, social networks

The article looks at online content creation by young people which can involve individual, communal (creating with existing networks), and collaborative activities (co-creating with strangers) online, thus disturbing the boundaries of public and private. Blogs and vlogs can be seen as parts of identity performance, networked individualism, and an act of making a private agenda public. In some cases such content creation represents exisiting face-to-face networks and can be seen as a form of communal activity, while in others content creation happens on shared platforms (e.g. Wikipedia) creating an 'affinity space' where strangers contribute based on a shared interest.

The authors argue that blogs can serve as identity performances, where both publicity and audience are important and children engage with a range of connections – from closest friends, to local communities, to global audiences of 'strangers'. Still young people see their blogs as their own partly intimate spaces and enjoy the opportunity for making new connections. Communal ties can create privacy in online communication based on the shared history of following someone's blog.

Privacy can be challenging: 'achieving privacy on networked publics requires special skills and digital and media literacy, such as understanding the differences between unmediated and mediated communication, online affordances, and various privacy tactics' (Oolo and Siibak, 2013: no page). Other challenges arise from the fact that the internet is not a unified platform and various privacy features exist with providers changing the existing settings over time, making control over one's privacy an on-going and complicated task requiring digital media literacy. This makes the less skilled or younger children more vulnerable to privacy risks than those who understand better how to control their privacy and identity and how online affordances shape the online public space.

51. Pradeep P and Sriram S. (2016) The Virtual World of Social Networking Sites: Adolescent's Use and Experiences. *Psychology and Developing Societies,* 28: 139-159.

Age: 13-18 [categorised as 12-15, 16-19]
Privacy Type: interpersonal
Data Type: data given
Method: survey
Country: India
Study Focus: behaviours
Platform: SNS

With the increased smartphone use and improved internet penetration in India, more young people are now online and use social network sites. The internet affords new opportunities for information-seeking, quick connection to others, independence, self-representation, social suport and well-being. Social media platforms play such an important part in young

people's lives that 'most of the developmental and mental tasks of adolescents are now being processed and negotiated there, especially in the domains of identity formation, peer influence, relationship management and social and emotional development' (Pradeep and Sriram, 2016: 145). The survey with 121 participants demonstrates that young people belive that social media helps them to feel more open and friendly (60%), to feel connected (58%), or to form new friendship connections (43%), strengthen exisiting teis with friends (40%), and even to discover one's own likes and dislikes (26%), to feel loved (22%), or incontrol of one's life (17%). The majority of young people in the study preferred online communication to face to face (71%), for example because it gave them more time to plan their answers (48%). Young people tended to post more when they were happy (73%) and also compared themselves to others (their photos, number of friends, status messages, and wall posts). Gilrs' SNS activities were controlld more by their parents than boys' (56% vs 44%) as were younger teens (69% of the 13-15 years old group vs 31% of the 16-18 group). Girls were also more likely to be friends with their parents on Facebook (59% vs 41% of boys). There were important gender differences in the privacy-related behaviurs as well: girls were more aware of ways to keep personal details safe, used SNS privacy settings more often, were less likely to contact strangers online, and were more concerned that their profile pictures might be misused.

52. 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: 414-426.

Age: 8-11 [categorised as 8-11]
Privacy Type: interpersonal, institutional, commercial
Data Type: data given
Method: participatory
Country: Canada
Study Focus: literacy
Platform: SNS

The article discusses a participatory research projects aiming to explore children's understanding of privacy and involve them in privacy literacy game creation (The Watchers). The authors argue that we live in a context where online and offline identities are blurrred: 'Many uses of the internet today, and social media in particular, depend on, or readily lead to, disclosure of people's 'actual' identities, situating them in known contexts and leaving limited separation between digital and physical presentations and performances of self' (Raynes-Goldie and Allen, 2014: 415). This is also a dymanic environment – what might appear private can suddlenly become public and management of privacy is a complicated and ongoing process in which children are perceived to be 'naïve experts'. While prominent online users, children often struggle to understand the

complexity of privacy online, particuallry in relation to its commercial aspects. While there is a concern about children's online privacy, most initiaties (government legislation, educational programs, or parental control applications) are based on adult perspectives and do not facilitate the development of children's autonomous understanding of privacy. Privacy literacy skills need to be learned independently by children, rather than taught and need to reflect the actual concerns and expereicnes of children. Autonomy is also linked to a range of developmental areas – identity formation, independence, responsibility, resilience, pro-social behaviour, trusting relationships critical thinking – which are also important for privacy literacy. Actively engaging children in content creation can boost their privacy skills: 'the engagement of children as research and design participants can lead to more successful approaches in the development of privacy literacy' (Raynes-Goldie and Allen, 2014: 414). The process of learning need to include both personal experience and scaffolding of the learning situation.
The findings suggest that children are aware of the importance of privacy and take measures to protect it (e.g. not using actual characteristics when creating online avatars) including from institutional survelliance. Privacy risks are mainly associated with the 'stranger danger' but not with commercial use of data. Children also had gaps in their capacity to decide which sites are trustworthy and to understand the privacy terms and conditions. The game aims to address these and develop privacy literacy without mentioning the internet at all but implicitly referring to: data shadows, information gathering and aggregation by large companies; and the use of personal information for marketing purposes. The game is ralated to everyday decisions children make about online privacy and aims to increate the ability to assess privacy risks and make judgements and decisions.

53. Redden SM and Way AK. (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.

Age: 12-18 [categorised as 12-15, 16-19]
Privacy Type: interpersonal
Data Type: gven
Method: FGD
Country: USA
Study Focus: behaviours, beliefs
Platform: SNS
Children's engagment with the internet is seen as a negotiation of tensions between risks and rewards of praticipating online and the choices that they had to make. The study idrntified five types of tensions: 1) Staying connected vs disconnecting: they structured their lives around being connected and experience tension when forced by circumstances to disconnect; 2) Desire for freedom vs oversight or constraint: the children

wanted autonomy but also had to abide to parental rules or netiquette. They were tailoring their messages based on platform and audience and posted content with care. There was a difference between older and younger teens in relation to parental involvement – younger teens assumed that parents were monitoring what they do and treid to navigate this supervision by selecting more private 'venues' such as a second secret account that the parents did not know about. Older teens saw less parental involvement and their choices aorund parental rules involved more reliance on personal experience or negotiation of the consequences of not following the rules (e.g. agreeing with adults when called out to avoid their anger). 3) Carefully curated online persona vs authentic self: positive affirmation motivated teens to put a lot of effort into content creation, they 'demonstrated an acute awareness of image management and post optimization' (Redden and Way, 2017: 29). They removed content they did not like (e.g. old embarrassing pictures, tags, comments) and trimmed audiences when needed and shifted focus from one platform to another. While putting a lot of effort into how they appear online, they also felt the tension of wanting to appear authentic and effortless. 4) Managing online and offline identities: the children often commented that their online representations are different from face-to-face ones (more currated, bolder, expressing more, easier to get misinterpreted) and used fake names, non-resembling avatars, and disabled geolocation to protect their identities. Still, online communication was seen as strengthening offline relationships. Generally they did not communicate with strangers or disclosed information only after a period of initial trial. 5) Participation vs resisting the onlien culture: teens were critical of caring about getting likes (but also enjoyed the attention), posting sexual content (al children disapproved and knew the dangers, even some who had done it), and online bullying but still engaged in these activities. It seemed that teens found it easier to ignore bad behaviour than report or confront it (e.g. being a bystander). When they resisted the online culture, it was to protect their identity or friendships. All these tensions were ongoing negotiations rather than non-reconcilable dichotomies. Finally, the authors point to a number of practical implications from adopting a 'tension-based approach', including the need to cultivate digital empathy and give empathetic advice reframing the fear-based responses to the digital.

54. Shin, W., & Kang, H. (2016). Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet. *Computers in Human Behavior, 54*, 114-123. doi:10.1016/j.chb.2015.07.062

Age: 12-18 [categorised as 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: survey
Country: Singapore

Study Focus: support and guidance, attitudes, behaviours
Platform: General

This study explores the role of parents and the Internet in adolescent's online privacy concerns and information disclosing behaviour. Literature suggests that parents affect how adolescents use and are influenced by the Internet. Study underpinned by parental mediation theory and parental knowledge theory. Research question: *which type of parental practice increases or decreases adolescents' privacy risks online?* Examines how parental mediation (efforts to mediate Internet use) and adolescents self-disclosure (adolescents taking to parents about Internet experiences) are associated with adolescents' online privacy-related perceptions and behaviours (privacy concerns, willingness to disclose personally identifiable information, and actual disclosure of personal information online). The study also examines the role of the Internet- prior studies suggest that higher levels of Internet use can increase chances of engaging in risky online behaviours. The study also investigates which type of Internet activity increases privacy risks among adolescents.

The authors adopted Westin's (1967, see above) conceptualisation of privacy. The study acknowledges the significant purchasing power that adolescents wield, and their subsequent emergence as a consumer segment of interest for marketers and especially so online. Cookie-placing, location-based advertising, and behavioural targeting are used by marketers to collect personal information from adolescents to reach and appear to this target audience. They also encourage adolescent consumers to disclose more personal information in exchange for enhanced online communication experiences (Shin and Kang, 2016: 115). 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. Restrictive mediation refers to parents' limiting access to media or rule-setting about appropriate media context or exposure. Instructive 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. Literature suggests that instructive mediation, by virtue of its critical discussion and engaging in dialogue, is more effective. Restrictive mediation (control-based) can be effective in reducing risks associated with adolescents' online use, but too much can cause boomerang effects. Sasson and Mesch argue that restrictive mediation is similar to notions of 'control' and 'solicitation', while instructive mediation is viewed as similar to child disclosure in supporting autonomy and parent-child dialogue. Kerr and Stattin (2000) identified three key sources of parental knowledge: child disclosure (free and willing disclosure), parental control (efforts to control adolescents' freedom without explaining rules and restrictions), and parental solicitation (gathering information about children by asking children themselves or others). While all contribute to parental

knowledge, child disclosure is suggested as the best source of knowledge, and a significant predictor of adolescents' good adjustment.

Hypothesis 1: Instructive mediation will be more effective than restrictive mediation in a) increasing concerns about online privacy and b) decreasing online information disclosure among adolescents.

Hypothesis 2: The amount of time adolescents spend on the Internet and their engagement in online communication activities will be a) negatively associated with concerns about online privacy and b) positively associated with information disclosure online.

Privacy concerns were measured using three, five-point Likert surveys (self-administered) with 746 adolescents (12-18 years) in four secondary schools (52% male respondents, mean age 14.3, did not specify but inferring then 48% female, no mean age given). Survey items for privacy concerns were adapted from Pew Internet's Teens' Privacy Survey (2012). To measure information disclosure, behavioural intention (personally identifiable information- PII- items adopted from COPPA guidelines) and actual disclosing behaviour were measured (adapted from EU Kids Online).

Restrictive mediation was measured by asking respondents to rate how often the adult they spent most time with at home monitored and controlled their Internet use (adapted from prior research on parental mediation). Instructive mediation was measured by asking respondents to indicate (yes/no, dichotomous format) whether the adult they spent most time with at home helped on or talked about proper ways of using the Internet (adapted from prior work on parental mediation).

Adolescents' disclosure to parents measured by asking how often they talk to parents about what they have seen on the Internet (five-point Likert). Engagement in online communication activities was assessed by asking respondents how often they play online game with other people on the Internet, visit a social networking site, and chat with people online (five-point scale).

Findings suggest that instructive mediation is more effective in reducing privacy risks- negatively associated with intention and actual disclosure of personal information. Gels with self-determination theory, where supporting children's autonomy facilitates children's perceptions that following parental expectations is self-determined. Adolescents who frequently talked to their parents had heightened privacy concerns, which may indicate heightened awareness. Adolescent internet use plays positive and negative roles- amount of time spent online and involvement in SNS is positively associated with online information disclosure. Online chatting was positively associated with heightened privacy concerns (controlled for demographic variables- not explained what they are). Peer-relatedness can have substantial influence of social behaviours,

including online information management. The study found that adolescents' privacy concerns are not associated with information disclosing behaviour, which can be explained by the privacy paradox.

While adolescents' self-disclosure to parents was associated with online privacy concerns, it was not associated with the behavioral outcomes; and parental mediation perceived by adolescents (especially instructive mediation) was associated with the behavioural outcomes (willingness to disclose PII and actual information disclosure), it was not associated with the perceptual outcome (privacy concerns). These findings may imply that different parental practices are associated with different socialisation outcomes and goals.

55. Steijn, W. M. P., & Vedder, A. (2015). Privacy under Construction: A Developmental Perspective on Privacy Perception. *Science Technology & Human Values, 40*(4), 615-637. doi:10.1177/0162243915571167

Age: 12-19 [categorised as 12-15, 16-19]
Privacy Type: interpersonal, commercial
Data Type: given, data traces
Method: online survey
Country: Netherlands
Study Focus: media literacy, attitudes
Platform: General

This article introduces notion of privacy conceptions- individuals' specific ideas of privacy- suggesting that differences in privacy concerns between young and old are due to the different developmental life stages based on questionnaire data amongst adolescents (12-19), young adults, (20-30) and adults (31+). Study found that the different areas on concerns are also reflect the strongest relationships to the concerns. Uses Vedder's four dimensions: relational, spatial, decisional, informational.
Authors argue against the notion that young people are less concerned about privacy compared to older people. Instead, they hold that informational liberality of youth and the supposed lesser privacy concern is explained by more subtle reasons. The authors focus on cognitive aspects of privacy (i.e. what is it) in addition to the affective (what are your privacy concerns).

Use developmental perspective to underpin study- adolescents' developmental goals are important for the articulation of the privacy conceptions. Argue that the focus of their privacy conception is their vulnerability to their parents' intrusions. The internet and SNS may be an opportunity to escape parents' scrutiny, rather than seen as a privacy risk.

Results show that young people do report less privacy concerns compared to older people- but adolescents associate relationships with privacy unlike young people and adults who are more likely to associate privacy with data collection, profiling, identity theft etc. The reported lower privacy concerns can be understood as a property of growth that is like to shift in the future. While adolescents were able to associate privacy with the situation involving relationships, fewer adolescents were able to associate it with informational privacy- data mining, profiling etc. This focus on relationships aligns with developmental need to pursue new friendships out of reach of known adults who control/manage most other aspects of their lives. The results from the young adult cohort reflect that this (and adolescence) is a transitory space.

Adolescents also do not have strong association of privacy with data collection concerns- author hypothesise this is because adolescents are not yet targets of banks, employers, government agencies; especially as this shifts for the young adult cohort.

56. Third, A., Bellerose, D., Diniz De Oliveira, J., Lala, G., & Theakstone, G. (2017). *Young and Online: Children's Perspectives on Life in the Digital Age (The State of the World's Children 2017 Companion Report)*. Retrieved from: https://www.westernsydney.edu.au/__data/assets/pdf_file/0006/1334805/Young_and_Online_Report.pdf

Age: 10-18 [categorised as 8-11, 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: Participatory
Country: Global
Study Focus: media literacy, attitudes
Platform: General

Main messages give strong overview of the report. Underscores children's concerns about commonly discussed online risks, as well as the reliability of access to the Internet, parental intrusion into their 'private' lives online, and their digital literacy skills. Adolescents are attuned to tensions between their desire to engage, and protect themselves, and responsibility to others. Tend to possess understanding of and strategies for addressing risks encountered online. Suggest that children's framings of the internet and digital technology echo mainstream conceptualisations and discourses which can limit their imaginations.

Methodology: 490 children 10-18 from 26 countries participated in UNICEF country office workshops- distributed data gathering (see: RERights methodology http://doi. org/10.4225/35/5a248c6b047e5). Individual and group-work to collect data in a participatory manner.

57. Wisniewski P, Jia H, Xu H, et al. (2015) "Preventative" vs. "reactive": How parental mediation influences teens' social media privacy behaviours. Association for Computing Machinery, Inc, 302-316.

Age: 12-17 [categorised as 12-15, 16-19]
Privacy Type: interpersonal
Data Type: given
Method: Secondary Analysis
Country: USA
Study Focus: media literacy, support and guidance, strategies
Platform: General

The study is based on a secondary analysis of the 2012 Pew Research Center's Internet and American Life Project's Teens and Privacy Management Survey of 588 US-baed teenagers (age 12 – 17) and one of their parents. The study found that 81% of parents were worried about their child's online privacy. The study distinguishes between two types of parental intervention – direct parental intervention (reflecting technical and restrictive mediation and including the use of parental controls, setting the child's privacy settings) or active parental mediation (instructive or monitoring behaviours including talking about posting practices and reviewing or commenting on existing posts). The authors also identify two types of teen privacy behaviour on social media: 1) Privacy risk-taking incuding 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 stranges, regretting posting onine content, automitic lication sharing); and 2) Privacy risk-coping involving seeking advice or angaging in safety behaviours such as posting fake information, deleting content, blocking or delting contacts, deactivating one's account.

Socially developing adolescents are engaged in making difficult decisions about information disclosure and their parents are involved in dynamic decision-making about which parenting privacy stregeties to adopt. Parents who were more concerned engaged more in privacy measures but the different strategie sthey use had different effect on their children's behaviour. 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 they were also less likely to engage in safety behaviours. Based on this, the authors conclude that seeking advice does not always 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 showed higher level of concern as well 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 info). Teens associated only risky interventions with higher privacy risk, which in turn was linked to advice-seeking and coping behaviours, while sensitive information was assocciated only with coping behaviours and basic infomrtaion was not linked to either perceptions of higher privacy risk or coping behaviour. Based on this, the authors suggests that teens have mainly retrospective behaviour when it comes to privacy risks.

The authors use the data to identify four types of parenting privacy practices: "unengaged parents," whose engagement in direct intervention or active mediation is low; "highly engaged parents" who demonstrate high levels of intervention in both and two 'middle' categories: "controlling parents," who display high direct intervention but low active mediation; and "counselling parents" who have low direct intervention but high active mediation. Controlling parents had the most suppressive effect – reducing privacy risk, corrective behaviours but also frequency of use of SN and the network complexity of their children. Active medition was found to be more empowering as children angaged with SN more, experinsed some risk bit also engaged in coping behaviours. This was observed particulrly strongly for the children of highly enagged parents who had high enagegement and complex social networks, despite the restriction from direct parental intervention (it is unclear why children of counselling parents didn't do better than highly engaged parents, this is not discussed in the text). None of the parent styles were effective in reducing contact with strangers, possibly because the children did not disclose this with their parents.

58. 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

Age: no age
Privacy Type: interpersonal, commercial
Data Type: given, data traces
Method: Secondary Analysis
Country: USA
Study Focus: media literacy, support and guidance
Platform: General

The notion that teens are at risk online due to their poor decisions related to privacy and information disclosure is prevalent in the litarature, the solution often seen as increasing their privacy concerns. While restrictive online practices reduce privacy risks, they also reduce the online benefits and do not teach teenages to effectively protect themselves online. A parent-centred appraoch, however, reinforces exisitng priviledges (perhaps this refers to more skilled parents?) and also leaves out the most vulnerable groups of children, such as foster children. The exisitng research evidence demonstrates that children value their privacy and

engage in protective strategies, while also appreciating the ability to engage online. Teens seem to perceive privacy risks 'as a learning process' (Wisniewski, 2018: 87) taking measures when risks have escallated to a potentially harmful situation but forecloing these risks limts children's autonomy and ability to develop.

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 conrol (prioritising long-term consequences over short-etrm desires), and risk coping (addressing an encountered problem in a way that reduces harm, whichis influenced by teen's and parental risk perception). The author analysed 75 commercially available mobile apps on Android Play and found that overwhelming majority of features (89%) within these apps supported parental control (monitoring or restriction), rather active mediation. In addition, many of the apps were 'extremely privacy invasive, providing parents granular access to monitor and restrict teens' 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 expeirence them as restrictive and invasive. The way forward suggested by the author involves: encouraging teens to self-regulate their behaviour; designing apps base don teen's needs; safety features which do not compromise privacy (e.g. by giving parents access only to meta-level information and not the granular details).

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

Age: 12-17 [categorised as 8-11, 12-15, 16-19]
Privacy Type: interpersonal, commercial
Data Type: given
Method: Secondary analysis
Country: USA
Study Focus: a
Platform: General

Using a nationally representative survey with 800 teenagers aged 12 to 17 (Teens & Privacy Management Survey conducted by Pew Research Center's Internet & American Life Project between July 26 and September 30, 2012), the study investigates how demographics characteristics, frequency of use and size of social network sites (SNS), types of online contacts, trust, and privacy control influence teenagers' self-disclosure on SNS and regret. Privacy is defined as 'one's control over his or her personal information and determination of when, where, to whom and to what extent such information to be disclosed' (Xie and Kang, 2015: 401, drawing on Westion, 1967).

SNS encourage users to disclose personal information (photos, videos, contact details, interests, etc) but disclosing too much information and unauthorised access to it (by advertisers, employers, parents) can lead to regret. Younger people are more likely to regret their posts (27% of people over 25 compared to 54% of under 25 have regretted their posts according to Croteau, 2013 and over 20% of the younger users have removed posts to avoid damage). The existing research suggests that older teens disclose more personal information than younger teens and adults and boys do so more than girls. More frequent SNS users and people with wider networks are also more likely to share more but the relationship between the type of online contacts and disclosure is controversial. The evidence related to the impact of privacy concerns on privacy protective behaviours is also mixed and demonstrating the paradox of people sharing information even though they have privacy concerns. The existing research demonstrates, however, that trust is amongst the most important factors influencing self-disclosure, including sensitive information, because it minimises the perceived risk.

The study found that large proportion of teenagers post a photo of themselves (91%), revealed their real name (91%), personal interest (85%), birth date (82%), place of residence (71%), current school (69%), and relationship status (60%). About half (52%) posted their e-mail address, and about 1 in 10 posted their mobile phone number (20%) and videos of themselves (25%). Older teens and those with public profiles disclosed more information, boys shared more personal information (school name and phone number) than girls. Teens who are active users tend to disclose more personal identification information while those with more friends share more insensitive details (school name, relationship status and personal interests) and contact information. The likelihood of posting regret increases with frequency of use, network size, and having strangers as friends. Trust did not predict disclosure of insensitive information and personal identification information but was associated with disclosure of contact information. Overall, teens either tend to share more on public profiles or share less regardless of who the audience is but the study did not find any relationship between regret of posting and privacy settings or self-disclosure. 'Easiness of usage, ubiquitous functions, and user-friendly features of privacy setting interface may reinforce teens' privacy protection behaviour. Given teens' literacy and computer skills, they may not understand the privacy policies or have the ability to adeptly change their privacy settings' (Xie and Kang, 2015: 405).

60. Youn S. (2008) Parental Influence and Teens' Attitude toward Online Privacy Protection. The Journal of Consumer Affairs, 42: 362-388

Age: 14-18 [categorised as 12-15, 16-19]
Privacy Type: interpersonal, commercial
Data Type: given

Method: ex-post facto
Country: USA
Study Focus: strategies, media literacy, attitudes, support and guidance
Platform: General

The study investigates how parental involvement influences children's privacy concerns and strategies looking at different mediation styles and their effects on privacy protection. Drawing on consumer socialisation framework, the teens' understanding of consumer behaviour is seen as influenced by 'socialisation agents' like parents, peers, educators, mass media. The authors conceptualise privacy as based on the ability of the individual to control their information and the terms under which it is collected, disseminated, accessed, and used but acknowledge that this is not achieved in a consumer environment. The existing research suggests that higher level of privacy concern is associated with strategies to handle privacy risks, likelihood to read privacy messages, and providing less personal information, and expecting negative consequences from information disclosure.

The level of concern increases when people become aware of misuse, accessibility to sensitive information, and when risks outweigh the benefits. According to the Teenage Research Unlimited (2006) 37% of teens are not worried about misuse of information and 20% thought it was safe to disclose personal information on networking sites or public blogs. Pew (Lenhart et al., 2005) found that only 21% were concerned about privacy breaches.

The study distinguishes between socio-oriented communication (encouraging conformity to family values and including parental monitoring and control of children's consumption) and concept-oriented communication (children are encouraged to express views and gain decision-making skills), as well as three types of mediation– rulemaking, co-viewing, and discussion. The research found that family communication patterns affect teenagers' perceptions of privacy-related parental mediation, which then affect privacy concerns and the formulation of privacy protection measures. Teens with socio-oriented communication had more family rules and co-used the internet with parents. Teens with concept-oriented communication tended to talk with parents more about commercial privacy. Rule-making did not create higher privacy concern but co-using the internet and discussions resulted in higher privacy concern. The teens who were more concerned about privacy also supported government regulation, school education, and wanted the right to be forgotten (name removal request). Rulemaking and co-surfing led to support for government regulation. Rulemaking and discussion were associated with support for education at school. Right to be forgotten was not associated with any parental mediation style.

Note: primary research with ex-post facto design (survey with 395 secondary school students from a public school; USA; Shortcomings: parental mediation measures not standardised

61. 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

Age: 12-13 [categorised as 12-15]
Privacy Type: interpersonal, commercial
Data Type: given
Method: survey
Country: USA
Study Focus: strategies, media literacy, attitudes,
Platform: General
The article draws on survey data of 141 middle school students (12-13 year olds) in the USA- an age group on cusp of being protected by COPPA and not being protected as they transition. 61% of respondents were girls, 39% boys. The author uses Rogers' (1975. 1983) protection motivation theory as theoretical framework, identifies determinants of adolescents' privacy concern levels, and how that affects their privacy protection behaviours, particularly e-marketers' information collection practices. Roger's theory suggests that individuals' assessments of risks and benefits associated with risky behaviour plays a pivotal role in motivations to protect themselves from such behaviour. It also posits that self-efficacy (belief in one's capability to successfully carry out an action) is essential for explaining protective motivation.
Based on this and the literature, the author developed a conceptual framework for understanding young adolescents' privacy concerns: interpersonal sources (gender, internet use, persuasion knowledge, privacy knowledge) and cognitive appraisals (vulnerability to risks, info disclosure benefits, privacy self-efficacy) affect levels of online privacy control, which result in privacy protection behaviours (fabricate, seek, refrain).
The data show that perceived risks of information disclosure increased privacy concerns, but perceived benefits of information exchange showed a decrease in privacy concerns. Risk-coping behaviours were affected by privacy concerns as adolescents seek interpersonal advice (from parents, teachers), additional information (reading privacy statements), or avoid using certain sites requiring personal information. Young adolescents' concerns over online privacy is affected by threat appraisals, and privacy education can increase adolescents' awareness of technological solutions or tighter privacy settings as coping and threat-mitigating strategies.

Privacy self-efficacy did not strengthen level of privacy concerns- possibly as young adolescents' confidence in their ability to protect their information from e-marketers may mean they have little concern about the negative consequences associated with information disclosure. It may also be because they do not have a fully developed understanding of

Internet use and its pitfalls, which may bias their privacy self-efficacy optimistically.

62. 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: 157-165.

Age: 16-19 [categorised as 16-19]
Privacy Type: commercial
Data Type: profile
Method: experimental
Country: Belgium
Study Focus: strategies, media literacy
Platform: SNS (facebook)

The article explores the effect of retargeting advertising on adolescents' purchasing behaviour using an experimental design with exposure to both targeted and non-targeted advertising on Facebook. Privacy concern is measured via a six-point Global Information Privacy Concern scale developed by Malhotra et al (2004).[9] The study found that adolescents are overall more likely to purchase products after retargeting advertising than non-retargeting. However, as the privacy concern increased, so did the sceptical attitudes towards retargeting 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).

Note: primary research with an experimental design (363 adolescents aged 16-18 years from 6 different schools); Belgium; shortcomings: very marginal discussion of privacy concerns

63. Zhang-Kennedy L and Chiasson S. (2016) Teaching with an Interactive E-book to Improve Children's Online Privacy Knowledge. *Proceedings of the The 15th International Conference on Interaction Design and Children.* Manchester, United Kingdom: ACM, 506-511.

Age: 7-9 [categorised as 4-7, 8-11]
Privacy Type: interpersonal
Data Type: given
Method: quasi-exp
Country: Canada

[9] Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4), 336-355. http://dx.doi.org/10.1287/isre.1040.003

Study Focus: media literacy
Platform: e-books

The study explores the effectiveness of an interactive e-book (Cyberheroes) for educating children aged 7 to 9 about online privacy risks. The book introduces privacy-related issues such as protection of personal information, online trust, location sharing, cyberbullying, and passwords, digital trail via a storyline involving superheroes trying to maintain their secret identity on the internet after losing their privacy-related cyber-powers. Privacy proficiency tests were carried out (using Wilcoxon signed-rank tests) showing significant improvement in children's privacy knowledge and retention after one week.

64. 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.

Age: 7-9 [categorised as 4-7, 8-11]
Privacy Type: interpersonal, commercial
Data Type: given
Method: experimental
Country: Canada
Study Focus: strategies, media literacy,
Platform: e-books

The article discusses the research summarised in Zhang-Kennedy and Chiasson (2016) with the addition of a control group where text-only version was used while the treatment group used the e-book. The privacy proficiency test contained four knowledge-based questions and six scenarios-based questions assessing children's privacy-conscious behaviour. For example, the password scenario used for the pre- and post-test was: "Your best friend wants to borrow your password to email a funny picture to a friend that you both know. What would you do? Why?". The results show that, while children in both groups had a significant increase in privacy proficiency over time, the text group's positive outcomes decreased one week after the reading. The authors conclude that "images and interactive elements in ebooks support children's knowledge acquisition, retention, and transfer" (transfer relates to applying the knowledge to a similar situation) (Zhang-Kennedy et al., 2017: 17).

Notes: primary research with quasi-experimental design (22 parents and children aged 7-9 years reading the e-book or a text version; pre- and post-test and a one-week follow-up test); Canada

Bibliography

Abbas R and Mesch GS. (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.

Agosto DE and Abbas J. (2017) "Don't be dumb-that's the rule I try to live by": A closer look at older teens' online privacy and safety attitudes. *New Media & Society,* 19: 347-65.

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

Bakó RK. (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 CM. (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 LR and Spenser KA. (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.

boyd d and Marwick AE. (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: Chowdhury G, McLeod J, Gillet V, et al. (eds) *Transforming Digital Worlds. iConference 2018. Lecture Notes in Computer Science.*: Springer, Cham, 442-52.

Children's Commissioner for England. (2017a) Growing up digital. A report of the Growing Up Digital taskforce London Children's Commissioner for England.

Children's Commissioner for England. (2017b) 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., 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 SH 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 GN. (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 VP, Rutledge SA, Bagdy LM, 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 KW. (2013) Profiling high-school students with Facebook: how online privacy laws can actually increase minors' risk. *Proceedings of the 2013 conference on Internet measurement conference.* Barcelona, Spain: ACM, 405-16.

Emanuel L and Fraser DS. (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, USA: International Communication Association, 1-27.

Gelman SA, Martinez M, Davidson NS, et al. (2017) Developing digital privacy: Children's moral judgements concerning mobile GPS devices. *Child Development,* 89: 17-26.

Ghosh AK, 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: 81-87.

ITU and UNICEF. (2015) Guidelines for Industry on Child Online Protection.

Kumar P, Naik SM, Devkar UR, 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.

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 School of Economics and Political Science.

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

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, 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: 1-22.

Marchionini G. (2008) Human–information interaction research and development. *Library and Information Science Research,* 30: 165-74.

Martin F, Wang C, Petty T, et al. (2018) Middle School Students' Social Media Use. *Educational Technology & Society,* 21: 213-24.

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, Colorado, 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 DM 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 SY. (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 NF. (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.

Ogur B, Yilmaz RM 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.

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.

Peter J and Valkenburg P. (2011) Adolescents' online privacy: toward a developmental perspective. In: Trepte S and Reinecke L (eds) *Privacy online.* Heidelberg: Springer, 221-34.

Pradeep P and Sriram S. (2016) The Virtual World of Social Networking Sites: Adolescent's 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 SM and Way AK. (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.

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.

Steijn WMP and Vedder A. (2015) Privacy under Construction: A Developmental Perspective on Privacy Perception. *Science Technology & Human Values,* 40: 615-37.

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.

UKCCIS (2015) Child safety online: a practical guide for providers of social media and interactive services. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/487973/ukccis_guide-final_3_.pdf

Westin AF. (1967) *Privacy and freedom,* New York: Atheneum.

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.

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.

Xie WJ and Kang CY. (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.

Yu J, Hu PJH and Cheng TH. (2015) Role of affect in self-disclosure on social network websites: a test of two competing models. *Journal of Management Information Systems,* 32: 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 r-book to improve children's online privacy knowledge. *Proceedings of the The 15th International Conference on Interaction Design and Children.* Manchester, United Kingdom: 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.