Children's data and privacy online

Growing up in a digital age

Evidence review supplement: coded sources

Sonia Livingstone ▪ Mariya Stoilova ▪ Rishita Nandagiri

January 2019

LSE Media and Communications

ico. Information Commissioner's Office
Grant Recipient

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

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 a desire for information, friendship and communication, and is shaped by the user's social status and positioning, disposition, 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. They draw on Westin (1967)[1] 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)[2] (items include: 'I am concerned about my privacy when using a Facebook account', 'I am concerned about online organisations 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)[3] (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 gender differences were also 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

[1] Westin, A.F. (1967) *Privacy and freedom.* New York: Atheneum.
[2] Buchanan, T., Paine, C., Joinson, A.N. and Reips, U.D. (2007) Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology* 58(2), 157-65.
[3] Pan, Y. and Zinkhan, G.M. (2006) Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing* 82(4), 331-8.

concerns about privacy, but their own study found the opposite – higher collectivism was associated with more 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 aged 11-17 (n=24), the authors explore young people's understanding of their data worlds. They share preliminary findings from piloting a library-based learning experience to explore the links between social media behaviour and data traces. Interviews reflected young people's 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 part of their personal identity, yet rarely mentioned privacy or safety in relation to it.

The study draws on Marchionini (2008),[4] who refers to these data traces as 'proflections of self' – data traces of interactions created un/consciously that make up our collective, virtual selves. The 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. (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.

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. It draws on interviews with 11- to 18-year-olds (n=22) to explore their understanding and perceptions of data literacy, and their knowledge acquistion.

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

Teens' 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 people's 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 the internet through web browsing or social media applications, data plans or 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-targeting on platforms based on their use, connecting it to their sense of self/online personas. Respondents were aware that apps and online services could access their location information or other data, but did not apply privacy or rights lenses to it.

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

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 programme 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 young people remix, share and adapt their peers' media artefacts. Remix is an information behaviour and (digital) literacy skill learned over time, and part of 'participatory culture' (Jenkins, 2009).[5] The 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 (Ahn et al., 2012: 1).'

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 online identities visible to others. Their participation in these

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

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 they were explicitly afforded the option to create anonymous profiles, the 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, 127-34.

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: Social networking sites

Other existing studies on social media and privacy focus on security risks, but here the authors aim to offer a more balanced view of social media, exploring how young people use it as a source of communication. They 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, home address, school, as well as favourite activities, music and films, and about a fifth contained relationship information. This information was not always correct – some gave an earlier date of birth, others stated that they were married. Adding unknown people as friends was not uncommon.

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

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 (aged 12-18, n=418) in four Greek cities completed a self-reported questionnaire on internet use at home and types of parental supervision (in 2004-05). The authors found that internet access remains low and is an indicator of socioeconomic status (SES) stratification. It is insufficiently used for school purposes, but younger students (aged 12-15) used it more frequently for schoolwork 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 could 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 with 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, 2645-64.

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: Social networking sites (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 their 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 a 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 of use): Facebook, Twitter, Google+, Tumblr, Instagram, ASKfm, Skype, Snapchat, YouTube, WhatsApp and Kik. Students were given seven reasons to choose why they used these social networking sites. The two responses with the highest mean were: 'to keep in touch with family and friends' and 'to find information'. Students (8.3%) who said they did not use online social networking sites 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 social networking sites and privacy concerns were greater.

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

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: Social networking sites

The authors explore girls' (aged 15-17) and young women's (aged 18-22) 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 policy-makers' debates.

Findings suggest that girls are overlooked within policy and policy responses, relying on gender-neutral language and ignoring the sociocultural 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 architecture 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 – also infringes on their rights and privacies. They suggest that platform providers be 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, R.K. (2016) Digital transition: Children in a multimodal world. *Acta Universitatis Sapientiae, Social Analysis* 6, 145-54.

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

Using 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- to 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, email, game downloads and in using tablets – needing little to no guidance. The authors conclude that children are comfortable with using smart devices, experiencing them daily, and that they are immersed in multimodal technological environments. Despite this, they are narrow,

routine users who do not fully understand 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. (2018) 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: Social networking sites

Using an online observational, ethnographic approach (observing 14- to 17-year-olds' Facebook and AskFM profiles through 'friends of friends' settings), the authors suggest that teenagers engage in strategic privacy management as a tactic to increase their social and symbolic capital. They contend that in order for teenagers to show their peers that they're no longer children, they represent their private lives in public spheres.

The 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 as a surrender of their privacy itself. Intimacies are also seen within an 'exchange market', where teenagers bargain and exchange intimate information based on their assessment of its value. These social bonds are used as commodities, which are 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, C.M. (2014) 'I had no credit to ring you back': Children's strategies of negotiation and resistance to parental surveillance via mobile phones. *Surveillance and Society* 12, 401-13.

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 the perception that all children should be accountable and accessible at any time and any 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. Efforts to create a 'risk-free environment' are challenged as unrealistic and unachievable. Risk aversion restricts children's play, development and agency, and constrains their exploration of physical, social and virtual worlds.

This article explores strategies employed by children in middle childhood (aged 8-12, n=60, 32 girls, 28 boys) 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). The field site was an Irish town classified as 'urban', with several housing developments/estates that most children in the area reside in. The estates did not have formal communal seating areas or fixed play equipment. Participatory data collection techniques were utilised, such as visual photography and participant observation in two single-sex schools and in the housing estates over one school year. Photo elicitation group discussions were held after the photographs were collected and reviewed.

The findings reflect that children in middle childhood play close to their home, where parents rely less on mobile phones and more on alternate systems of surveillance. Some children reported having mobile phones for 'emergencies', but were unsure what these would constitute, and instead recounted specific instances (parents checking or confirming their location/movements), lending weight to parents monitoring children in time and space, allowing a feeling of control and minimising risk perception. The children, however, understood that the phones were tools for textual rather than oral communication. They also employed strategies of negotiation – they were actively engaged in planning their own movements and in an ongoing dialogue of compromise with their parents (texting instead of calling, for example). They also used strategies of resistance (pretending the phone was on silent, that it had run 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 example). Texting language – use of specific characteristics or codes – may be incomprehensible to adults, limiting their ability to comprehend the texts even when they're read, allowing the children a resistance to their monitoring.

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

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

Eleven- to 15-year-olds report feeling vulnerable as social networking sites require relinquishing personal information to fully engage in these spaces. However, some felt that this default expectation of disclosure engendered feelings of privacy violation. It also meant they wished for greater control over their privacy settings. Participants discussed changing privacy settings, but were also aware of their interactional nature – despite their own privacy settings, others with less stringent settings could make them vulnerable. They also discussed the tension between needing to maintain privacy and yet engage in social media spaces. Despite being aware of the potential risks, they continued to use social media as these risks were perceived to be low and happening to 'other' people. If, however, they did encounter a risk, it would shift how they 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 teens' 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 (aged 11-18) data literacy. Data literacy is understood as the awareness of data-related rhetoric and data flows. This study forms 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.

The 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 linked data to digital contexts. Teens had a broad understanding of the lifecycle of data, particularly the beginning and end of the cycle, but little knowledge of data flows and infrastructure. While aware of the security issues related to social media, they spent little time thinking more broadly about the digital traces of their data and implications for their future selves.

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

Age: N/A
Data type: Given

Privacy type: Institutional
Method: Interviews
Country: USA
Study focus: Data literacy, interface, attitudes
Platform: General

The authors explored how families perceive the storage and handling of their data (personal data, relationships, school records and academic results, social support and benefits, employment, housing, criminal records, GP and medical records, library usage) by state welfare and civic authorities, using game-based interviews. The study found that families often consider their data as 'personal' and want to be in control of it (especially in relation to information perceived to be 'sensitive'). This was often prompted by recognised risks (of a criminal, medical, welfare, social and psychological nature) and fear of the consequences of mishandling or misuse of the data.

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

Age: 'Teenagers' (14+, but does not specify 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 that 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.

The 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 – they 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 where '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 are seen as a form of information flow/control. The teens highlight the importance of control and personal agency, and their struggle to assert control, especially when technology usurps or undermines their agency/control. Teens are aware of and acknowledge the lack of control in relation to those who have power over them – parents, for example – who violate the boundaries that the teens create or assert. While their engagement online is 'public', taking their images or text out of context (for an assembly on 'privacy', for example) 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.

Teens' take on democratic and social roles (allowing them to make sense of the world and their relationship to society) but are often restricted from entering some spaces (publics) they wish to enter, which can thus push them to create their own publics - which networked publics often are). The authors use Nancy Fraser's[6] 'subaltern counterpublics' to understand practices of young people engaged in resisting and challenging adult-imposed discourse or authority (and to explore their own identities and interests in relation/resistance to the norm). The social space of networked publics takes on greater significance as the teens' 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 and searchability – which require contending with dynamics not usually encountered in daily life – the imagined audience for their posts/performances, the collapse and collision of social contexts, and the blurring of public and private. How the social constructs of publicity and privacy are understood has 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. The authors assert that teens focus on what to protect rather than what they ought to disclose – a focus on exclusion which is considered 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 also what they might gain from this loss – a connection or a signalling of trust. They also utilise the multiple communication channels afforded to them, for example by using private dyad communication such as 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).

[6] Fraser, N. (1990) Rethinking the public sphere: A contribution to the critique of actually existing democracy. *Social Text* 25/26, 56-80.

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 a 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 are not engaged in 'bad' privacy practices[7] – this 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 to use language/specific references for their intended audiences.

16. 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, they 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 friends' lists. A substantial minority of children in the study reported being in online contact with someone they have not met in person. Children also reported being bothered by internet scams, pop-up advertisements and people sharing too much personal information online.

17. 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.

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

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

Study focus: Behaviour, attitudes
Platform: General

This study examines factors influencing preteens 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.

The authors define 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.' They use social cognitive theory and protection motivation theory to build a conceptual model for information privacy protection behaviour (i.e. behaviour influenced by gender, information privacy axiety, self-efficacy and perceived importance – all of which also influence each other). 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 (e.g. not opening emails from unknown senders and protecting personal information). Parents' privacy concerns affected behaviour positively. The 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.

18. 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, the 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 the age of 2 in developed countries have a digital footprint/online presence through their parents. A study conducted across 21 countries in Europe explores how children under the age of 8 engage with digital technologies, and parents/family members' perceptions and management of technology use.

The authors found that children's first contact with digital technologies and screens was at a very early age (below the age of 2), and often through parents' devices. Children learn to interact with digital devices by observing the 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 the age of 6, were social networkers, invited by their parents and generally integrated into a family account. Children did not have a 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 concerns.

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

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: Social networking skills

The study explores teens' affective, behavioural and cognitive states in relation to the personal data they generate on social media. It uses Ostrom's ABC model, which defines three components of attitudes as A – affect, B – behaviour and C – cognition. The ABC model explains the 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 displayed interest and curiosity 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 information, increasing security settings). Those who reported positive affects may rely on existing routines.

20. 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: Focus group discussions
Country: UK
Study focus: Attitudes, behaviours
Platform: Social networking sites

This report explores the social media lives of children aged 8-12 in the UK (n=32) to understand the impact of social media on 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 social media several times a day, unlike the younger children. Social media contributed to their happiness – silly videos, for example – and allowed them to be creative and play games. Children were also beginning to see offline activities through a 'shareable lens'. Parents and educators have successfully ingrained cautiousness in their children around online risks pertaining to predators and strangers, but the children were less aware of how to protect themselves from other risks affecting their mood or emotions.

21. 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. *5Rights*, 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. The scenarios included:

(i) *The right to know, a scenario about the kind of personal data that is 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. They 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 terms and conditions (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 concrete 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.* This scenario resonated with jurors, but they were split between those who believe that one ought to take personal responsbility for any 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 constrained recommendations. This also reflected jurors' lack of knowledge about data generated by or about them.

The 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, engendering 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 a broader curriculum that improves internet literacy.

22. 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: Focus group discussions, questionnaire
Country: USA
Study focus: Behaviours
Platform: Mobile phones, laptops and tablets, social networking sites

This 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 that 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 the 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 and adminitrators – were able to access their social media behaiour, making them uncomfortable.

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

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)
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.

Institutional privacy: 60% of survey respondents disagreed that governments have the right to know all personal information about them, but this shifted when asked 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' – the authors interpreted this to mean that they were unsure which they valued more or that they valued them equally. Fifty per cent strongly agreed/agreed that the internet should be free from control by governments and big businesses. Respondents did not receive much MIL training relating to privacy – 56% said it was addressed for one hour or less over an entire course.

This report draws parallels between Cannataci, Zhoa, et al.'s (2016)[8] analysis of three pillars of privacy, transparency and freedom of expression, and likened it to rights to privacy, freedoms of expressions and of information. The authors highlight the constantly shifting interplay between the three pillars and these rights, where the values surrounding them are constantly in flux. The authors suggest that an awareness of the commodification and monetisation of personal profiles and an understanding of the duties of institutions in cyberspace are key compotents of privacy competencies, and are valuable for the construction of privacy.

24. 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: Social networking sites

This empirical study explores middle school students' ('tweens', aged 10-14, n=42) online privacy practices. It investigates their online activities including texting, use of mobile phones, Instant Messaging (IM), playing games and social networking sites (Facebook and Myspace). Participants reported that they were under-age users of social networking sites.

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 or family members. Tweens mentioned institutions such as the police or government less frequently. One participant mentioned advertisers ('spammers'). In terms of privacy management online, participants relied on withholding

[8] Cannataci, J.A., Zhao, B., Torres Vives, G., Monteleone, S., Mifsud Bonnici, G. and Moyakine, E. (2016) *Balancing privacy and transparency and redefining their new boundaries in the internet ecosystem*. UNESCO Series on Internet Freedom. Paris, France: UNESCO.

or proactive strategies. *Withholding strategies*: Nearly all participants discussed withholding content from online spaces, first considering the (in)appropriateness of the information they posted, 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 unaware of privacy options.

Participants said they turned to close relations for advice on managing their own/others' online privacy, and checked before posting photos. Three teens created explicit privacy guidelines with friends and family. They also discussed '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 social networking sites and other platforms based on the belief that the site designers and developers had 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 of being online, given this particular age group.

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

Age: 12-18 [categorised as 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Questionnaire, focus group discussions
Country: Australia
Study focus: Behaviours, attitudes
Platform: Social networking sites (Myspace)

This study compares the level of information disclosed by young (aged 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. The 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.

The 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 questionnaire also measured viewpoints on the drivers of information disclosure, and the value of privacy to the user. They also conducted two focus group discussions (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 in 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 in as they mistakenly believe it is mandatory or because its template and page set-up appears to influence disclosure. Signalling suggests that the more the user wants to portray themselves in a certain light, the more likely they are to disclose information, and this 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.

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

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: Social networking sites

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 three-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 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 use more private spaces for private exchanges than those afforded by social networking tools.

Student communities included personal communities (groups students belong to outside school – church groups, sports groups, etc.) and the school community (school-based clubs etc., including friendship groups). There were differences in which tools were used to connect with different communities – such as Instagram or GroupMe for group activities like team sports to enable a shared online space. While other tools such as 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.

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

Age: 'Secondary school' – 14-18 [categorised as 'teenagers']
Privacy type: Commercial
Data type: Profile
Method: Experimental
Country: USA
Study focus: Interface/design/settings
Platform: Social networking sites

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), fuelling large-scale and highly personalised spear-phishing attacks, and exposure to perpetrators of child sexual abuse and violence.

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

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. The authors emphasise that identity is multifaceted, including physical and personality attributes as well as behaviour patterns that identity has multifaceted- 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 email or an 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 example, 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 had been posted online. Unintended sharing of personal information by 'friends' in online settings was perceived to be the biggest threat. The diverse social networking sites used were not seen to offer privacy protection with overlapping friend networks and services that link together different social networking site accounts, making compartmentalisation difficult. Blurry digital and physical divides were due to the ubiquitousness of technology, as communication via tablets and smartphones in physical environments was parallel with private messaging in online platforms. Concerns with this bridging were around connecting physically based information (phone number, for example) to cyber-persona (email id, for example), but the same level of concern for the reverse was not present.

Avatar design workshop (where participants design an avatar, fill out a 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 the majority settled on features similar to their own. Some suggest that this was so their friends could recognise them, but also 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. They admitted using other identifiers such as favourite colours or background pictures related to their interests, but did not view this as linking 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.

29. 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.

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: Social networking sites (Facebook)

This study uses the Pew Research Center's Internet and American Life Project's Teens and Privacy Management Survey to explore socialisation agents related to teens' concern about online privacy and the relationship between teens' level of concern and their privacy behaviours. Analysis shows use of social networking sites and parents' privacy concerns as motivating factors in teens' increased privacy concern, driving the adoption of privacy-setting strategies.

The authors use Westin's (1967)[9] conceptualisation of privacy to frame the study, including the shift in public trust in information collection activities by government and other agencies, pushing privacy to a first-level social issue in the USA. This complements Lessing's (1998)[10] understanding of privacy as what is left over after removing what can be monitored and what 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 the Children's Online Privacy Protection Rule (COPPA) doesn't cover marketers collecting voluntarily shared information on social networking sites, teens are likely to be unaware of the implications, and this is a cause for concern. Parents' roles as socialisation agents is emphasised as they shape young people's consumer norms and marketplace knowledge.

Results showed that parents were concerned about marketers 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. Social networking site usage was another socialisation agent that increases teens' privacy concerns about marketers, as increased media use is related to the development of consumer knowledge and scepticism. Female and older teens tended to spend more time on social networking sites. 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 are more likely to set their profile to private or partially private if they are concerned with privacy.

30. 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

[9] Westin, A.F. (1967) *Privacy and freedom.* New York: Atheneum.
[10] Lessing, L. (1998) *The architecture of privacy*. Available at http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf

This study explores how young people (aged 13-17) negotiate online friendships and online privacy concerns. The 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 about 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 are task-oriented. Affective friendships reflect a deep appreciation for the other and are generally seen as irreplaceable, as well as friendship- 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. They explained conscious and thoughtful decision-making processes about sharing personal information, largely based on the relationship they were attempting to support or build. This suggests that rather than concluding that the privacy paradox reflects a lack of knowledge or that teens prioritise socialisation over privacy, teens do not treat friendship (e.g. their online interactions) 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 that 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, see 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.

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

Age: 4-10 [categorised as 4-7, 8-11]
Privacy type: Interpersonal
Data type: Given, traces
Method: Experimental
Country: UK
Study focus: Behaviour, literacy
Platform: Wearable technologies

This article discusses the use of ThinkActive, a system aiming to encourage primary-aged school children to reflect on their own personal activity data. ThinkActive includes activity trackers and pseudonymous avatars to encourage children to reflect on their physical activities either privately or to share the data selectively with others. The study reports that the personal data is an asset to children as they can compare their results with others and contribute to the success of their teams. The privacy allowed by the avatar is also encouraging children to engage and allows them to 'socially negotiate access to their identity' (Garbett et al., 2018: 9) based on friendships and judgements of trust.

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

Age: 8-9 [categorised as 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 the age of 3, children have firm understandings of property rights – that non-owners may not use others' objects without permission. By ages 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 via a mobile GPS device.

Each experiment demonstrated how GPS mobile devices functioned and the children were asked to judge the acceptability of someone else tracking their possessions or them tracking someone else's. Experiment 1 examined reactions to tracking a device (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 had placed it on an object. The experiments differentiate between perceived implications of tracking and implications of violating one's personal space by physical contact.

The experiments found that the youngest children (aged 4-5) did not appear to evaluate the use of mobile GPS devices 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 old, 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 moral considerations were invoked to explain their beliefs. Yet, children were more accepting of this behaviour than adults, focusing on the benefits of object tracking. The authors suggest that a possible reason for this difference may be that 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 on negative outcomes themselves. The 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.

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

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 disclosure and visibility – networked privacy (Marwick and boyd, 2014)[11] refers to disclosure within friendship circles on social media platforms; Nissenbaum's (2004)[12] theory of privacy as contextual integrity refers to the negotiation of privacy norms and cultures; and the communication privacy management theory (Petronio, 2002)[13] 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 relation to children, decisions are often limited (e.g. 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 (they resembled parental stalking and felt disrespectful) and did not facilitate communication or trust between parents and children. There were positive comments that reflected children's appreciation of helping control undesirable practices (related to time spent, concentration and pornography), which helped them feel safer.

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

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 strategies, attitudes?
Platform: Social networking sites

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. It draws on literature that suggests teenagers have more difficulty than adults in resisting temptation where incentives are present, and young adolescents are less concerned about potential risks of information disclosure. The study uses Westin's concept of information privacy, and suggests that in

[11] Marwick, A.E. and boyd, d. (2014) Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16(7), 1051-67.
[12] Nissenbaum, H. (2004) Privacy as contextual integrity. *Washington Law Review* 79, 119.
[13] Petronio, S.S. (2002) *Boundaries of privacy: Dialects of disclosure*. Albany, NY: SUNY Press.

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. The authors found a direct positive relationship between perceived behaviour control and disclosure, suggesting that information disclosure is informed, in part, by availability of opportunity.

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

Age: 12-18 [categorised as 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Survey
Country: Belgium
Study focus: Privacy strategies
Platform: Social networking sites

Privacy literature (Eliison et al., 2011; Wilson et al., 2012)[14] highlights three strategies for privacy management on social networking sites: (i) disclosure management; (ii) application of privacy settings to information disclosed; and (iii) audience management. Previous research shows that in some cases users may deliberately self-censor to protect privacy. Customisable privacy settings can allow users to divide posts on social networking site platforms into separate privacy spaces, but have also been criticised for engendering a false sense of privacy as the size and composition of a network has a bearing on levels of privacy. The study is framed by Altman's (1997)[15] multi-mechanic privacy theory, where privacy is a network of behavioural mechanisms that people utilise to achieve desired levels of social interactions. People adopt a mixture of privacy-protective mechanisms that operate interdependently. In this study, the authors examine whether the three strategies work independently or as interdependent mechanisms for adolescents' privacy strategies.

Results show that the majority of respondents engage in audience management by restricting their profiles to friends only. Yet, a few adolescents use more fine-grained settings to divide friends' lists into groups with varying privacy settings. Findings suggest that the more adolescents used social networking sites for getting acquainted with people, the more inclined they were to disclose their personal data. The longer they've been active users, the less inclined they are to use privacy settings. Those who reported using social networking sites for meeting new people tended to apply less privacy settings unlike those interested in extending their social networks. The more frequently adolescents

[14] Ellison, N., Steinfield, C. and Lampe, L. (2011) Connection strategies: social capital implications of Facebook-enabled communication practices. *New Media and Society* 13(6), 873-92; Wilson, R., Gosling, S. and Graham, L. (2012) A review of Facebook research in the social sciences. *Perspectives on Psychological Science* 7(3), 203-20.
[15] Altman, I. (1977) Privacy regulation: Culturally universal or culturally specific. *Journal of Social Issues* 33(3), 66-84.

disclosed personal data, the less likely they were to use privacy settings to protect this data and the more friends they reported having on social networking sites – suggesting that Altman's multi-mechanic privacy theory also applies to privacy regulation in online spaces. Age, however, was not found to be significantly associated with the outcome variables, that is, age did not affect their privacy behaviours and trends were observed across all age groups. The study concludes that teenagers' privacy management is based on what they decide they're willing to disclose, the settings they choose and the audience that can access their information.

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

Age: 14-15 [categorised as 12-15]
Privacy type: Interpersonal
Data type: Given
Method: Secondary analysis
Country: The Netherlands
Study focus: Privacy strategies (?), behaviours
Platform: Social networking sites (Facebook)

This study investigates whether peer influence processes, popularity and trust predict Facebook privacy settings. Findings suggest that peer influence affects privacy settings, with imitation processes particularly pronounced in classroom settings that are highly connected. Popularity is also related to privacy settings. More popular adolescents are more likely to maintain public profiles, which may be due to a need for self-expression and status maintenance. Girls, minority ethnic members, younger adolescents and pupils in lower educational tracks are more likely to opt for private profiles, which suggests lower levels of trust in 'most others'.

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

Age: 12-16 [categorised as 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Unstructured questionnaire interview (?)
Country: China
Study focus: Privacy behaviours
Platform: Social networking sites (Renren)

The authors explore adolescents' use of social networking sites and their privacy and security behaviours, and the associations between their online behaviours and psychological and developmental factors. Findings suggest that adolescents were likely to use their real names and photos, but their privacy disclosure behaviours were influenced by age, gender, personality and attachment styles. The authors grouped online behaviours into utilisation, socialising and privacy disclosure. Older adolescents were found to exhibit more utilisation behaviours in contrast to younger

adolescents, who showed more socialisation behaviours.

The authors found that attachment styles were important for predicting online privacy disclosure behaviour, where insecure attachment is associated with less self-disclosure on social networking sites. Intrapersonal factors were also important as older adolescents were more familiar with the features of social networking sites and socialised less, which may be partly due to more complex and gradated understandings of privacy.

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

Age: 12-17
Privacy type: Interpersonal
Data type: Given
Method: Secondary analysis
Country: USA
Study focus: Privacy behaviours
Platform: Social networking sites

The authors conducted a secondary analysis of the Pew Research Center's survey, testing two theoretical models (risk-centric, concern-centric) of adolescents' information privacy behaviours. Teens' risk-taking behaviours are multi-dimensional and interrelated, where not all risks are equal and there may be a pattern of risk escalation. Risk-taking behaviours may also be cumulative, where lower risk-taking levels may be predictive of higher risk levels. Findings suggest that a 'risk-centric' framework may be more useful that a 'concern-centric' framework. A 'risk-centric' framework suggests a risk escalation process wherein online disclosures can make one susceptible to risky online interactions, which are associated with higher levels of privacy concern. These privacy concerns can predict advice-seeking and remedy/corrective risk-coping behaviours. The authors distinguish between risk-taking behaviours and risk-coping behaviours within privacy behaviours. A 'concern-centric' framework accentuates privacy concerns in determining risk-related behavioural outcomes. The risk-centric model embodies an experiential learning process, allowing risk-taking behaviours to be understood as learning opportunities for the development of risk-coping behaviours (i.e. 'risk-as-learning' process). The findings also suggest that teens are capable of identifying risks, and attempting to manage low-level risks on their own and turning to external support for higher-level risks, which may tie in to their developmental learning processes.

The authors challenge the applicability of the privacy paradox to this age group, as it may not be the privacy component that fails to moderate behaviour, but the mismatch between conceptions of risk. Privacy concerns are not effective motivators of risk-coping, but potentially a mediating factor underlying risky behaviours. The authors suggest that rather than viewing risk management as insulation from risk, exposure to privacy risk and subsequent coping mechanisms may be viewed as part of their development as digital natives. They suggest that enhancing risk awareness can help teens' learning processes.

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

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

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

40. Lapenta, G.H. and Jørgensen, R.F. (2015) Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday* 20.

Age: High school?
Privacy type: Interpersonal, commercial
Data type: Given, traces
Method: Ethnography, focus group discussions
Country: Denmark
Study focus: Attitudes/beliefs, strategies
Platform: General

This study attempts to reformulate the concept of 'online privacy' within current polict debates, centring the concerns of young people and their perceptions, negotiations and control of online spaces. In policy debates, online privacy tends to be understood as a form of protection of users' legal right to privacy or a protection of the liberal self. Discussions have also centred around the shift in privacy environments with the advent of the internet – that privacy is no longer a social norm. However, the authors refute this assertion, using evidence based on youth opinions/responses, even in contexts where online sharing is the default.

Findings show that respondents were reflective of their self-representation, controlling not just their own posts but also that of their parents and friends about them. Respondents used privacy tools available on the platform, but were also conscious of its limitations. Respondents also relied on online social norms to manage their privacy and posting behaviour, remaining responsive to the requests or

comments to delete photos of friends or others. Social media, while acting as an infrastructure for young people's everyday lives, is still seen as an integrated part of their identity rather than an entire representation. Social networking sites – Facebook in particular – were also the primary channel of social information and communication.

Respondents were asked to reflect on their knowledge and assessment of risk relating to surveillance and commercial use of data. While reflexive and aware of their presentation, it was harder for them to reflect on instututional privacy, commercial data use, mining and surveillance. Many had not read the terms and conditions of the platforms they use, and suggested that to use social media one may have to give up some rights to data and content. The social value of these platforms was perceived as significantly larger than their potential risks.

Respondents had limited knowledge of commercial use of their data, showing little concern about any future use of their personal data and finding it difficult to conceive that it would be of interest to anyone. They perceived commercial social media platforms as primarily with a public and social infrastructure, even when they were aware of them as private businesses that control the terms of use and data use. Respondents sign off on privacy rights due to a specific framing of the service (i.e. framing of a commercial provider as a public service as part of the public sphere or as a commercial service) whilst utilising it in a different type of framing. In terms of surveillance, respondents believed it was less of a concern for them and more for those in totalitarian states, but agreed that it was unpleasant to consider.

The authors conclude that respondents envisioned two types of privacy: firstly, related to data shared voluntarily as part of their 'social privacy', and secondly, relaed to the repurposing of their data (mining, commercial use) seen as a precondition for social participation (removing the notion of voluntary engagement). The authors hold that the primary model for social media use is the 'consent model', but the structural conditions in which practices evolve and shift the sense of control and implementation of people's privacy rights must also be considered in policy discussions.

41. 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 children in the UK aged 13-16 and their use of social media found that teenagers form 'zones of privacy' using different channels for disclosure of personal information in a way that allows them to maintain intimacy with friends but also to sustain privacy from strangers and sometimes, parents. Their behaviour on social media demonstrated the shaping role of social

expectations in their peer group and their own understanding of friendships and intimacy on privacy norms and behaviours.

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

Age: 9-16 [categorised as 8-11, 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Interviews and focus groups
Country: Czech Republic, Romania, Spain, UK
Study focus: Attitudes/beliefs, strategies
Platform: Social networking sites

Privacy plays an important part in what Sonia Livingstone calls 'social media literacy' – literacy that encompasses platform affordances (including privacy-related), communication (creating and decoding it) and social interactions (e.g. relationships, privacy, anonymity). The development of this social media literacy is related to children's cognitive and social development, and while this argument is not made directly in relation to privacy-related competences, it would be interesting to research its application in this area. While children under the age of 11 do not express wanting to keep their online activities private, from 11 years onwards they develop a desire for independence from their parents. At a younger age (9-11), children's sharing of personal data is guided by parental advice (warning about strangers, paedophiles, exposure to unwanted content), but at an older age (11-13) children begin to experiment more and enjoy 'risky opportunities', but also learn how to make decisions about online trust and the consequences of 'wrong' decisions (e.g. about sharing information). Children's engagement with online platforms becomes more dynamic, including switching between different accounts on the same social media, making their digital footprint much more difficult to manage. Aged 14-16, children begin to develop a critical distance from their earlier sharing practices, more independence from parental or teacher mediation, greater awareness of the consequences of online behaviour and more knowledge of how to navigate platforms, audiences and privacy settings to create the desired balance of public and private. Social relations are competently managed online via blocking, deleting and amending contacts and content. Greater intimacy, albeit with fewer friends, and closeness (sometimes expressed via sharing passwords) become more important.

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

Age: 9-16 [categorised as 8-11, 12-15, 16-19]
Privacy type: Interpersonal, commercial
Data type: Given, traces, profiling
Method: Survey
Country: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, France, Germany,

Greece, Iceland, Ireland, Italy, the Netherlands, Norway, Poland, Portugal, Slovenia, Spain, Sweden, UK
Study focus: Behaviour, media literacy
Platform: General

While concerns about privacy risks and abuse of personal data are on the rise, particularly in relation to the increased use of mobile devices, there is still a lack of research evidence and sufficient policy efforts in this area. As children become more mobile and begin to use the internet from the privacy of their bedrooms, parents increasingly decide to trust them and not to invade their privacy. At the same time, children struggle with a range of privacy-related issues including reading and understanding privacy policies, knowing the public/private boundaries of online platforms and managing the privacy settings of the services and devices they use. This calls for better media literacy, regulation and interface design.

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

Age: 13-14 [categorised as 12-15]
Privacy type: Interpersonal
Data type: Given
Method: Observation
Country: UK
Study focus: Behaviour, media literacy
Platform: General

Based on a study of a London-based secondary school class, the book explores how adolescent learning and identities are being shaped by the digital world. Privacy should be understood as having control over one's information, rather than keeping information secret in a context where 'commercially owned networks are becoming ever more important in once-private processes of identity' (Livingstone and Sefton-Green, 2016: 7). Children had their own understanding of privacy based on their own practices and circumstances – sharing passwords was sometimes seen as a sign of closeness, but it also meant that a very private account can be seen as public while more public-facing accounts can be private if nobody else has access to them.

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

Age: 9-16 [categorised as 8-11, 12-15, 16-19]
Privacy type: Interpersonal, commercial
Data type: Given, traces, profiling
Method: Survey
Country: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Iceland, Ireland, Italy, the Netherlands, Norway, Poland, Portugal, Slovenia, Spain, Sweden, UK
Study focus: Behaviour, media literacy
Platform: Social networking sites

Social networking sites offer new possibilities for identity expression and social connection, and require children to learn how to manage the balance between privacy and intimacy. Most children

socialise online with people they know offline, but boys are more likely than girls to be in contact with people they only meet online (31% of boys and 20% of girls). Social networking sites offer opportunities for self-expression – 50% of 11- to 16-year-olds find it easier to be themselves online and 32% are able to share private things that they do not talk about offline. Most children keep their profile fully private (visible only to friends) or partially private (friends of friends), with less than a third of children (26%) having a public profile. On average, children share three of the six types of personal information they are asked: 14% share their address or phone number (7% in the UK) and 16% show incorrect age (21% in the UK). In countries where more children have a public profile, they also share more personal information, and in countries with more 'private' cultures, children have a private profile and also share less.

46. Livingstone, S., Ólafsson, K. and Staksrud, E. (2013) Risky social networking practices among 'underage' users: Lessons for evidence-based policy. *Journal of Computer-Mediated Communication* 18, 303-20

Age: 9-16 [categorised as 8-11, 12-15, 16-19]
Privacy type: Interpersonal, commercial
Data type: Given
Method: Survey
Country: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Spain, Sweden, Turkey, UK
Study focus: Behaviour, media literacy
Platform: Social networking sites

Following the boom of social media use and the increase of online hurtful behaviour, certain measures have been put into place to remedy this – limiting social media use to children agd 13 and over, designing social networking sites for children, introducing more advanced privacy settings and the opportunity to change the default settings, introducing report functionality and content moderation and more state regulations. The evidence regarding the effectiveness of these measures is still inadequate. The study found that the use of social networking sites by underage children is higher in countries lacking effective age restrictions and for those children whose parents impose no restrictions (even though the effect of parental regulations decreases with age). Generally, older children, girls in particular, are more frequent internet users; children who use the internet in their own bedroom and those whose parents put no restrictions on social media use were more likely to have a profile. Among social network users, 43% keep their profiles private to all but friends, and 28% have profiles that are part public, part private, allowing friends of friends to see them. Country differences are substantial, ranging from public profiles for 50% of children in Hungary to only 11% in the UK. The survey responses show that few children provide personal information online: only 11% revealed their address and only 7% reveal their phone numbers.

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

Age: 9-16 [categorised as 8-11, 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Survey
Country: UK
Study focus: Behaviour, media literacy
Platform: General

Over half of children aged 9-16 (58%) know how to change their privacy settings, with older children being more likely to know how to do this. Children in the UK are much less likely to have a public social media profile than their European peers (11% in the UK compared to 26% across Europe), with younger children, girls and children from a high socioeconomic status (SES) being more likely to guard their privacy online. Children in the UK are also much less likely to share their address or phone number (7%, compared with 14% in Europe), and more likely to show incorrect age (27% compared with the Europe average of 16%).

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

Age: 9-16 [categorised as 8-11, 12-15, 16-19]
Privacy type: Interpersonal, commercial
Data type: Given
Method: Survey
Country: Belgium, Denmark, Ireland, Italy, Romania, Portugal, UK
Study focus: Behaviour, media literacy
Platform: General

The levels of digital media skills are rising slowly – between 2010 and 2014 there was an increase in the proportion of children who know how to change their privacy settings (43% of 11- to 13-year-olds in 2010 and 55% in 2014) and how to delete their browsing history (37% in 2010 and 53% in 2014). Still, inequalities by gender, age and country remain, with many children lacking sufficient digital literacy skills. Fewer children talked about private issues online in 2014 (22% of boys and 24% of girls) than in 2010 (31% of boys and 27% of girls). Social networking sites are relatively safer in Ireland and the UK than in other European countries – profiles are more likely to be private, children start using social media later and when they do, they have fewer online contacts. Some recommended measures include content classification, age-appropriate privacy settings and easy reporting mechanisms.

49. 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, and explores some of the risks they face on social media (Facebook, Bebo and Twitter), including bullying, inappropriate contact, overuse, addiction and invasion of privacy. Invasion of privacy 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.

50. Madden, M., Lenhart, A., Cortesi, S., et al. (2013) *Teens, social media, and privacy*. Washington, DC: 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 social networking sites

A survey of 802 teens show that they now share online more personal information about themselves than in the past, including posting photos of themselves (91%), 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 that are designed to encourage sharing, as well as by the changing norms around sharing online and socialising. Sixteen per cent of teenagers automatically include a 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 and 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 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 and 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 teens – 17% of the 12- to 13-year-olds are 'very concerned' vs. 6% of the 14- to 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.

51. 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: Social networking sites

The study explores the practices of and motivations behind photo tagging (perceived usefulness, positive and negative aspects and tagging preferences) of Indian youth. The method used is described as a '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' (Malik et al., 2015: 12), as many girls saw tagging as unnecessary or as an intrusion of their 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.

52. 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: Social networking sites

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 social networking profile earlier on, and to check their social media for updates much more often than boys.

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

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

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

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 is 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 the 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 quickly became 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, the 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 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 had 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 could say to the child and when it recorded.

55. 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: Focus group discussions
Country: Canada
Study focus: Attitudes, media understanding
Platform: General

Drawing on focus groups with 54 children aged 10-17, the authors discuss the participants' interpretation of privacy policies on a few favourite children's sites (they 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 the 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.

56. 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 this study looks at the different safeguards that can prevent preteens from accessing unsuitable online content. A sample of 112 websites that were identified as oriented toward children was analysed for the type of safeguards they contain. 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 and regulatory agencies); and (3) *barrier safeguards*, requiring parental approval (via email, phone or 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 warning and threat safeguards resulted in lower information disclosure levels while only a warning safeguard resulted in higher disclosure. Children whose parents were more actively involved in parental mediation tended to disclose less.

57. 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: Social networking sites

The article investigates the extent to which children know what type of profile information they disclose on Facebook and to whom, 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 could 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 underestimating 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 also explained with the complexity of the interface.

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

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- and concept-oriented family communication style, informative and normative peer influence, whether they have an email address and how often they are online (socialisation agents). Concern for privacy was measured using a 14-item 7-point scale originally developed by Sheehan and Hoy (1999),[16] 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.

[16] Sheehan, K.B. and Hoy, M.G. (1999) Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising* 28(3), 37-51.

The results of the study indicate that the concern for privacy was positively 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 trying 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 email accounts are more concerned about privacy. In turn, higher privacy concern was associated with requesting removal from email lists, reporting unsolicited emails or responding negatively to them, and providing inaccurate personal information.

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

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

The authors used an online survey with 331 parent–child (children aged 10-17) pairs (in the US) to examine preferences about what people share about children on social media. The study uses communication privacy management theory to demonstrate that tensions arise when parents and children do not coordinate the disclosure of personal information. Children prefer that parents share positive content about them, as well as reflecting a positive family life/relationship. Content reflecting negatively on a child's self-preservation and 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 permission more often than they do, and this was especially marked in younger parents.

Using this data, the authors 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 a child by parents that requires their approval) and learning preferences (permission-seeking mechanism allowing social networking sites to learn and adapt to preferences over time). The authors suggest that an engine could collect labelled content (including embarrassing content) to understand evolving preferences, directing tone (scanning posts for positive/negative text or expressions and prompting to confirm sharing), however the authors do not engage with privacy-related risks associated with this functionality.

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

Age: Average age 15.55
Privacy type: Interpersonal
Data type: Given
Method: Survey
Country: Ireland
Study focus: Behaviours, attitudes
Platform: Social networking sites

The study draws on communications privacy management (CPM) theory (developed by Petronio, 2002),[17] 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. Eighty-nine per cent had a Facebook account and 84% had accounts with between three to seven 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 of 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.

61. 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: Social networking sites

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 as 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

[17] Petronio, S. (2002) *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: State University of New York Press.

future, and develop detailed strategies for managing their audiences. At the same time, they are not engaged 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.

62. Ofcom (2017) *Children and parents: Media use and attitudes report.* Available at: 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 media literacy (aged 5-11, and media access of those aged 3-4) and parents' views of children's media use and their efforts to monitor/limit use. Online survey data was 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. They 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. They also report understanding advertising revenue through sponsored ads, but are unable to identify it accurately (even when the word 'ad' appears). They believe that Google plays an authenticating role, believing search results can be 'trusted' as a result. They report negative experiences, but have developed strategies to report or tackle online experiences.

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

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 privacy 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 online – 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.

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

Age: 10-14 [categorised as 8-11, 12-15]
Privacy type: Interpersonal
Data type: Data given
Method: Survey
Country: Turkey
Study focus: Behaviours
Platform: Social networking sites

Based on a survey with 4,261 Turkish students from middle and high school, the research explores the sharing practices of young people, looking at the importance of demographics and social support. The study found that children from larger cities, boys and older children 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 those who relied on family more.

65. 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 as 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 ongoing 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.

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

Age: 13-17 [categorised as 12-15, 16-19]
Privacy type: Interpersonal, commercial
Data type: Data given, data traces, data profiling
Method: Participatory
Country: Australia
Study focus: Behaviours, media literacy
Platform: Social networking sites

The authors argue that the conscious volunteering of personal information by users is only a fraction of the overall data gathered, with most children providing personal data passively and unconsciously when using online services such as social media, provoked by the platform design and configuration. While young people are paying for supposedly free services with their personal data, they are oblivious of the possible consequences that 'social data are an important component of decision-making in fields ranging from financial credit through to job recruitment' (Pangrazio and Selwyn, 2018: 1). Young people also seem to be more concerned about breach of privacy in relation to friend networks and by unknown actors (such as hackers, identity thieves and paedophiles) and less so about the re-appropriation of their data by commercial entities. Some commercial privacy concerns existed and were related to being tracked online, that all the data is stored permanently and they are unable to delete their data. Still the children demonstrated a 'pragmatic non-concern' about things they could not control – such as what friends might post or how commercial entities might use their data – exhibiting an 'intellectual detachment', having a vague awareness that they are affected by data profiling but remaining intellectually disengaged from this process due to the overwhelming and uncontrollable misuse of their data.[18]

Other young people thought that their data was not valuable to anyone, while others displayed some confusion or misunderstanding of what personal data means, of how exactly their data is collected (e.g. that their location is collected only when using the geolocation-enabled app) or believing that their data disappears after being sent. Some participants also exaggerated the abilities of companies

[18] An argument made initially by Obar, J. (2015) Big data and the phantom public: Walter Lippmann and the fallacy of data privacy self-management. *Big Data and Society* July–December, 1-15.

to find things about them (e.g. that their conversations are monitored at all times via the microphone on their mobile phone), but then they continued to use social media, mostly as they felt obliged to agree with the terms and conditions (which they also found hard to understand). When the children were asked to use an app that demonstrated to them the data implications of their social media use, new concerns arose: the precision of tracking their movements, the ability to collate and visualise the meta-data into a comprehensive list of things they had done and places they had visited, and the emotional analysis of their text and images (the latter was often found to be inaccurate, which was both frustrating and reassuring for young people). After being faced with their data shadow, the young people became more aware of the implications and consequences of their data sharing, but still did not feel that they could change their behaviour much – they saw targeted advertising as a default part of contemporary life, felt unsure how to avoid data profiling, experienced a contradiction with their desire to participate, and felt unable to invest the time needed to constantly check their privacy settings, resulting in a sense of powerlessness. The authors argue that even though children do not display 'an unwitting trust' in social media platforms and have 'a sense that data are reused and repurposed in myriad ways. Yet the design of social media makes it impossible – if not impractical –to think about data flows... Without transparency of these connections, it is hard to understand how data flows within the system, let alone manage these through their privacy settings' (Pangrazio and Selwyn, 2018: 9).

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

Age: 13-18 [categorised as 12-15, 16-19]
Privacy type: Interpersonal
Data type: Data given
Method: Survey
Country: India
Study focus: Behaviours
Platform: Social networking sites

With increased smartphone use and improved internet penetration in India, more young people are now online and using social networking sites. The internet affords new opportunities for information-seeking, quick connection to others, independence, self-representation, social suport and wellbeing. 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 believe that social media helps them to feel more open and friendly (60%), to feel connected (58%) or to form new friendship connections (43%), to strengthen exisiting ties with friends (40%), and even to discover one's own likes and dislikes (26%), to feel loved (22%) or in control of one's life (17%). The majority of young people in the study preferred online communication to face-to-face (71%), because, for example, 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 (via their photos, number of friends, status messages and wall posts). Girls' social networking site activities were controlled more by their parents than boys' (56% vs. 44%), as

were younger teens (69% of the 13-15 age group vs. 31% of the 16-18 age group). Girls were also more likely to be friends with their parents on Facebook (59% vs. 41% of boys). There were also important gender differences in the privacy-related behaviours: girls were more aware of ways to keep personal details safe, used privacy settings on social networking sites more often, were less likely to contact strangers online and were more concerned that their profile pictures might be misused.

68. 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.

Age: 8-11 [categorised as 8-11]
Privacy type: Interpersonal, institutional, commercial
Data type: Data given
Method: Participatory
Country: Canada
Study focus: Literacy
Platform: Social networking sites

The article discusses a participatory research project aiming to explore children's understanding of privacy and to 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 dynamic environment – what might appear private can suddenly become public – and management of privacy is a complicated and ongoing process in which children are perceived to be 'naïve experts'. Although prominent online users, children often struggle to understand the complexity of privacy online, particularly in relation to its commercial aspects. While there is a concern about children's online privacy, most initiatives (government legislation, educational programmes or parental control applications) are based on adult perspectives and do not facilitate the development of children's autonomous understanding of privacy. Privacy literacy skills need to be learned independently by children rather than taught, and need to reflect the actual concerns and experiences of children. Autonomy is also linked to a range of developmental areas – identity formation, independence, responsibility, resilience, pro-social behaviour, trusting relationships and 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 needs 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 surveillance. 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 in understanding the privacy terms and conditions. The game aims to address these and to 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 create the ability for children to assess privacy risks and make judgements and decisions.

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

Age: 12-18 [categorised as 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Focus group discussions
Country: USA
Study focus: Behaviours, beliefs
Platform: Social networking sites

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 have to make. The study identified 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 by parental rules or netiquette. They were tailoring their messages based on the 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 they tried 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 caught 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 or comments), trimmed audiences when needed and shifted the 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 curated, bolder, expressing more, easier to get misinterpreted) and used fake names, non-resembling avatars and disabled their 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 an initial trial period. (5) Participation vs. resisting the online culture: teens were critical of caring about getting 'likes' (but also enjoyed the attention), posting sexual content (all children disapproved and knew the dangers, even some who had done it), and online bullying, but they 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 to give empathetic advice, reframing the fear-based responses to the digital.

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

Age: 9-18 [categorised as 8-11, 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Survey
Country: Australia, Japan, Indonesia, Korea, Taiwan
Study focus: Attitudes, behaviours
Platform: General

Rimini and colleagues define child online resilience as 'the ability to avoid and overcome risky and harmful situations when online' (Rimini et al., 2016: 16), and see privacy protection strategies, such as adjusting privacy settings, as a form of resilience behaviour. They found that a third of the children in Asia and the Pacific they researched (33%) were very likely to change privacy settings to avoid unwanted content, and over half (52%) did not share their passwords with anyone; there were no pronounced differences between the countries. However, the differences in using software to filter or block content were more significant – children in Japan (47% likely vs. 29% unlikely) and South Korea (48% likely vs. 33% unlikely) are less inclined to use these than their peers in the other surveyed countries (on average 63% likely vs. 26% unlikely). Girls were overall much less likely to take 'provocative pictures' or 'undress in front of the webcam' than boys (88% replied with 'very true' compared to 76% of boys). Less than 1 in 10 children had experienced some form of misuse of personal information: 10% of children had had their password used without their permission and 9% had had their photos used. Younger children were less likely to have a response strategy than older teens, but were more likely to seek help in such situation (see table 20 in Rimini et al., 2016: 51).

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

Age: 7-18 children [categorised as 4-7, 8-11, 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Ethnography (interviews, observation, pre- and post-study questionnaires, including smiley-o-meters for children)
Country: USA
Study focus: Privacy strategies, parents
Platform: General

This ethnographic study explores children's understandings of online safety and parents' strategies for children's online safety. The study considers the design implications and privacy problems. The author suggests that while human–computer interaction literature differentiates between security (a

technical concern) and privacy (largely social concern), study participants do not make the same distinction. Parents understand children's safety as safety from external threats (predators, adult content and spyware) and from inadvertently revealing personal information.

The study was conducted in two phases: a pilot interview with seven households (16 individuals – 8 parents, 8 children) in a technology firm's offices, and using security software in people's homes; 12 households were interviewed (33 individuals – 14 adults, 19 children). Parents' rules can be categorised as: (i) rules explicitly prioritising PC use relative to other activities (e.g. chores first, fixed time limits on use); (ii) rules based on social norms or trust (e.g. avoiding adult sites or implicit expectations – 'you know what to do') – some families said they had no rules, making them implicit members of this category; (iii) rules protecting the computer from threats (e.g. don't click on pop-ups); (iv) blocking specific activities deemed 'risky' (e.g. don't add strangers to chat or IMs); and (v) blocking activities deemed threatening (e.g. no social networking sites, no online purchases). Rule-enforcing strategies were also categorised – monitoring children's actions with or without technological aids, using blocking technology for certain activities deemed risky or threatening, encouraging self-restraint and discussing safe behaviour, and discussing safe behaviour while encouraging curiosity.

The author suggests that design considerations include effective mechanisms for risk communication for children, considering children's online engagement as a site of identity creation. This will create privacy-respecting spaces for children and technology that caters to their reading levels and comprehension (and perhaps even to their (tech) illiteracy). A possible way of doing this is to design for networked maintenance across machines.

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

Age: 13-17 [categorised as 12-15, 16-19]
Privacy type: Interpersonal, institutional, commercial
Data type: Data given, data traces, data profiling
Method: Participatory, experimental
Country: Australia
Study focus: Behaviours, media literacy
Platform: Social networking sites

In addition to the data shared by individuals (posts, photos, videos), much more data is drawn from online activities (e.g. via cookies) and combined with information gathered offline by data brokers ranging from governments to supermarket loyalty cards. Many forms of data gathering happen without user awareness and are used to create user identities (profiling), classifications and to filter online content via algorithms: 'the digital marketing industry that uses these data is opaque and complex, meaning that the (re)usage, collection and analysis of personal data by other parties has many aspects and dimensions that are unknown to users' (Selwyn and Pangrazio, 2018: 1). This data gathering has been enabled via the rise of social media and smartphone use, allowing real-time tracking across platforms and locations. In addition, young people can feel apathetic and powerless to control their privacy and security. Drawing on critical data studies, the authors argue that: 'digital data is implicit in the operation of power in contemporary everyday life' (Selwyn and Pangrazio, 2018: 2),

and use the notion of 'personal data tactics' to discuss children's approach to navigating the digital ecology. Children were active on social media (mainly Snapchat, Instagram and YouTube), and considered themselves relatively safe even though many were uncertain about what others could see about them and the permanence of their online posts. They had little awareness of third parties, except 'stranger danger'. After using a specific app designed to demonstrate the gathering of personal data, the children became more aware and concerned about geolocation data (perceived as creepy, unsettling and invasive). They also found the data analysis inaccurate (assuming different interests, nationality, visited places), which was reassuring. They also did not object to being targeted by advertising, which was perceived as an acceptable element of mobile media use.

As part of the experiment, the children were able to adopt different response tactics – check the terms and conditions, research and report back on the commercial background of social media platforms, run ad-blocking, tracking and geo-spoofing software, or alter their selfies in a way that aims to confuse facial recognition and photo analysis. The first two activities enabled them to become more aware of data use and sharing, the business model and ownership of the services, while the latter two were seen as uninteresting or ineffective. The authors describe the experiment as relatively ineffective in provoking the participants to change their personal data practices due to the perceived lack of effectiveness of any alternative actions combined with lack of time and expertise. While the children were generally interested and concerned about online privacy, they also felt overwhelmed and annoyed, but did not feel empowered to make changes, and nor did they feel in control of their privacy, leading the authors to argue in favour of changes to the business model that not only make personal data use more transparent, but also enable children to engage more actively and agenticly with the online platforms rasing their critical awareness. Hence they conclude that 'young people cannot be expected to face these challenges on their own. The development of personal data tactics is perhaps better approached along collective lines' (Selwyn and Pangrazio, 2018: 11).

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

Age: 13+
Privacy type: Commercial/institutional
Data type: Given, traces
Method: Platform analysis
Country: USA
Study focus: Behaviour
Platform: Social networking sites

Schools and school districts in the US are using third party applications and software to monitor and track students' social media profiles and use during and after school. This article considers the policy and ethical issues of data monitoring by exploring four US companies (Geo Listening, Varsity Monitor, Snaptrends and Digital Fly). The monitoring is justified by school districts and governors as an attempt to tackle bullying, violence and threats by and directed at students. The article argues that the business imperatives raise ethical concerns about young people's right to privacy under a regime of commercial data monitoring.

Geo Listening views risk sites for schools, offering services to mitigate emotional or social problems. It monitors and analyses public social media posts made by students aged 13+, reporting – on a daily basis – those flagged as a cause for concern to school administrators. This includes posts that are considered against a school's code of conduct. Reports include screenshots of flagged posts, whether they were posted on/off campus, time and date and the user's name. The authors contend that the reports move from flagging posts reflective of harmful behaviour to students only towards actions that are harmful to schools themselves, shifting from an interest in the safety of youth to the protection of the school/school district.

Varsity Monitor specifically monitors college and high school athletes with athletic scholarships or other professional sports scholarships, where negative social media presence can affect these opportunities. The company suggests that monitoring posts is in the interests of parents and children, but also allows them to ensure that students uphold standards (reputational and contractual). Varsity Monitor claims to have a '360 view' of athletes' online behaviour. Their third party content monitoring also suggests they monitor those in the students' wider networks without the network members' knowledge or consent.

Snaptrends uses 'geofencing' – providing relevant or custom geolocation information – and analyses posts and messages to create a social media map of posts from these customised ('lens-covered') locations. It can alert officials in real time of flagged issues or posts. Digital Fly claims to monitor threats in real time to help prevent incidents. It allows the creation of 'watch lists' to which school districts can add keywords, users, groups or locations. It has a 'tip line' for anonymous tips to warn of future incidents, and an 'incident rewind' function where school districts can look for evidence after an incident has occurred. Concerns have been raised around watch lists, particularly around issues of social sorting and racial discrimination. No privacy policy was available. The authors describe the language in these organisations' privacy policies as 'privacy prevarication' (Shade and Singh, 2016: 5), in the context of data use by third parties. It is unclear if the businesses cross-reference their data with other records or information available, invoking Haggerty and Ericson's (2000) 'surveillant assemblage'.[19]

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

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 adolescents' online privacy concerns and information-disclosing behaviour. The literature suggests that parents affect how adolescents use and

[19] Haggerty, K. and Ericson, R. (2000) The surveillant assemblage. *British Journal of Sociology* 51(4), 605-22.

are influenced by the internet. The study was underpinned by parental mediation theory and parental knowledge theory. The 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 talking 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) 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. Marketers use cookie placing, location-based advertising and behavioural targeting to collect personal information from adolescents. 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. The 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 (2014)[20] 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)[21] 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 the 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 (aged 12-18) in four secondary schools (52% male respondents, mean age 14.3; did not

[20] Sasson, H. and Mesch, G. (2014) Parental mediation, peer norms and risky online behavior among adolescents. *Computers in Human Behavior* 33, 32-8.
[21] Kerr, M. and Stattin, H. (2000) What parents know, how they know it, and several forms of adolescent adjustment: Further support for a reinterpretation of monitoring. *Developmental Psychology* 36(3), 366-80.

specify but inferring, then, 48% female, no mean age given). Survey items for privacy concerns were adapted from the Pew Research Center'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 or talked about proper ways of using the internet (adapted from prior work on parental mediation).

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

The findings suggest that instructive mediation is more effective in reducing privacy risks – negatively associated with intention and actual disclosure of personal information. This 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 – the amount of time spent online and involvement in social networking sites is positively associated with online information disclosure. Online chatting was positively associated with heightened privacy concerns (controlled for demographic variables – it was not explained what they are). Peer-relatedness can have a substantial influence on 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 behavioural outcomes, and while parental mediation perceived by adolescents (especially instructive mediation) was associated with 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.

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

Age: 'Tweens' – 9-12, and their parents (tween–parent dyad)
Privacy type: Interpersonal, commercial
Data type: Given
Method: Survey
Country: Korea
Study focus: Strategies, parental mediation
Platform: General

The authors drawn on John's (1999)[22] research on consumer socialisation research, theorising that children move through three stages: perceptual (aged 3-7), analytical (aged 7-11) and reflective (aged 11-16). In the perceptual stages, children's knowledge and decision-making tends to be based on a single dimension, rarely integrating individual experiences into a generalised knowledge structure; they are unable to incorporate external perspectives and find it difficult to under the use of privacy information. In analytical stages, they are able to understand other viewpoints at the same time as developing their own: this is a transitional period to understanding the motivations and goals of advertisers in collecting privacy-related information. In the reflective stages, they have more adult-like skills and understanding of consumption and consumer scepticism. Consumer socialisation is a process by which children acquire and develop a broad range of consumption-related attitudes, knowledge and skills (Moschis and Churchill, 1978).[23] The internet, unlike traditional media, makes it easier for marketers to collect a range of personally identifiable information from children.

The study found no significant impact of parental mediation on tweens' disclosure behaviours, contrary to previous studies and findings. The authors suggest this may be due to the uniqueness of 'tweens' and their particular developmental stage, and parents' difficulty with knowing how to best protect them. The survey included questions on voluntary disclosure of personally identifiable information in general online activities, and disclosure on marketers' request. Older tweens confident about their internet skills and who differed in opinion on their parents' mediation were more likely to disclose information to commercial sites. This may be due to their increased confidence and low parental mediation (or ignoring set restrictions), but may also be accounted for by their age. However, while they may become more sceptical as they get older, age alone is not enough to make children more discerning of online privacy risks.

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

Age: 16-18 [categorised as 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Interviews and focus groups
Country: USA
Study focus: Behaviours
Platform: Social networking sites

Social networking sites are a primary mode of communication and a way of expressing identity and strengthening friendship ties. The experiences of young people varied from being concerned about privacy and adopting high privacy protection settings to others who were less concerned and more relaxed with their settings as they trusted the people in their online network. Overall, privacy was important to the children and their online activities were carefully thought through (e.g. what photos or status updates to post). They mostly interacted with people they knew personally or were friends of friends, but the number of online friends varied from 200 to 5,000. Just over half of all 21

[22] John, D.R. (1999) Consumer socialization of children: A retrospective look at twenty-five years of research. *Journal of Consumer Research* 26, 183-213.
[23] Moschis, G.P. and Churchill, G.A. (1978) Consumer socialization: A theoretical and empirical analysis. *Journal of Marketing Research* 15, 599e609.

participants preferred to exclude their parents from their online social networks as a way of maintaining their privacy. Most had private profiles with only their name and profile picture being visible to strangers, and some students also avoided using their real name so that this would not affect their university applications. The students also knew how to manage unwanted content (photos, tags) and expressed concerns about geolocation settings (which might alert burglars that you are not at home).

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

Age: N/A
Privacy type: Interpersonal, institutional, commercial
Data type: Given, data traces, data profiling
Method: N/A (three related Ottawa-based studies)
Country: Canada
Study focus: Attitudes, behaviours
Platform: General

Steeves and Regan (2014) point out that most educational programmes (e.g. European Union's Ins@fe initiative, myprivacy.mychoice.mylife, the 2013 campaign created by the Privacy Commissioner of Canada, 2008 and the US government's Kids.gov, 2013) refer to privacy as information control, advise children on the dangers of disclosing personal information and associate the lack of disclosure with safety. This not only creates the image of the online environment as dangerous and unsafe, but also does not correspond with children's own concerns. Instead, the authors suggest that privacy should be seen as 'an inherently social practice that enables social actors to navigate the boundary between self/other and between being closed/open to social interaction' (Steeves and Regan, 2014: 300). While children enjoy self-exposure to known and unknown audiences on a range of social platforms, they also hold a complex set of norms associated with who should access their information and how they should react to it, and feel discomfort when these norms are not being followed. Negotiating both privacy and publicity online, young people experience online communication as a forum for self-presentation, identity play and relatedness, often testing and exploring the boundaries of online disclosure. They also have expectations of how people will engage with their online information – while close friends are expected to be attentively following them online, parents are supposed to trust and not 'watch' their children online even if they can, and people who are not close friends should be less engaged with the online profiles. Lack of privacy, particularly from parents, educators and employers, can be resented by young people and seen as surveillance. Privacy and the ability to adjust their performance based on the various social roles young people play is essential and when various audiences collide in the online space leaving young people to feel vulnerable.

The authors identify four different understandings of the value of privacy by young people: (1) Contextual: privacy is guided by certain norms and values, often complicated by an evolving environment and disagreements with what these norms are, especially with adults. (2) Relational: privacy is at the centre of forming relationships that need to be based on transparency, mutuality and trust, but some online relationships that young people have (with school boards, marketers, potential employers or law enforcement agencies) are one-dimensional. The idea of consenting to online

privacy terms and conditions does not involve reciprocity; it forms a one-way relationship allowing the monitoring of the consent-giver who has no other option but to agree or be refused the benefit. These one-way relationships are purely instrumental and do not involve a process of negotiation:

> Current information privacy and data protection policies assume that information practices involve instrumental relationships – and hence do not protect, or take into account the possibility of, a social value of privacy. They fail to capture the continuing importance of privacy after one consents to collection and disclosure. They fail to reflect any reciprocal element after consent is secured or to embody the continual involvement of the data subject. Consent in this case is not consent to an ongoing relationship with an organization but consent to that organization taking and using information for its own purposes (Steeves and Regan, 2014: 306).

(3) Performative: this involves online self-discovery and role-play that allows both public and private identities to emerge. Privacy fosters and protects autonomy, self-development and a more authentic narrative – all of these are somewhat jeopardised when the online environment allows the instrumental and commercial invasion of privacy. (4) Dialectical: there is a dialectical tension between the public and the private spheres that have collapsed online, which means that young people can seek both privacy and publicity online at the same time. This means that privacy and consent have to be constantly negotiated and cannot be given away irreversibly. The authors conclude that the privacy policy needs to support the (transparent and equitable) negotiation of boundaries.

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

Age: 11-17 [categorised as 8-11, 12-15, 16-19]
Privacy type: Interpersonal, commercial
Data type: Given
Method: Survey and focus groups
Country: Canada
Study focus: Attitudes, behaviours
Platform: General

The authors emphasise the commercialisation of children's online activity and data, suggesting that: 'a number of scholars have argued that children's websites intentionally play on children's developmental need to communicate so that the sites can convert their social play into a tradable commodity (Steeves, 2006; Shade, Porter, & Sanchez, 2005; Grimes & Shade, 2005; Chung & Grimes, 2005), and that children are often naive about the commercialization of their information' (Steeves and Webster, 2008: 14). Parents in the USA and Canada have legal responsibility to ensure the online protection of their children's privacy, and the study found that parental supervision can reduce children's willingness to disclose personal information and can increase their privacy-protective strategies. Still, it is not sufficient to fully protect children's online privacy as this only reduces privacy risk-taking but does not eliminate it. Furthermore, children's understanding of online privacy protection policies does not seem to have an effect on privacy risk-taking.

Drawing on survey and focus group data with Canadian children aged 11 to 17, the article discusses the relationship between parental supervision and the protection of children's online privacy. Privacy is measured as the average score from two scales: on disclosure (the child's willingness to disclose private information in an online game, contest, chat room, free email account, online profile, blog) and on protective behaviour (if the child is likely to take privacy proactive steps such as reading privacy policies, not sharing passwords, not sharing private secrets online and seeing privacy protection skills as part of being a 'good internet user').

The survey found that large proportions of children were willing to disclose personal information such as a real name, address or email when engaging with different online activities: signing up for a free email account (76%), creating a social media profile (76%), posting on their blog (57%), entering a contest (56%), registering for a game site (69%), participating in a chat room or discussion forum (48%) or using a dating site (39%). Almost half of the respondents (49%) had never read the terms and conditions of the sites they visit and thought it was safe to share secrets via email and online messages (45%), and nearly a third (31%) had shared passwords with friends. The risky behaviour increased with age – at the age of 17 42% of children were willing to disclose personal information compared to 39% of the 15-year-olds and 21% of the 13-year-olds. At the same time, the older children were less likely to engage in protective behaviour – 38% of the 17-year-olds compared to 36% of the 15-year-olds and 26% of the 13-year-olds were classified as least likely to use protective behaviours. The older children were also more likely to report intentionally visiting websites with adult content (pornography) – 21% of the children aged 17, 18% of those aged 15 and 7% of those aged 13. Boys were also more likely to be willing to reveal personal information and less likely to engage in protective behaviours than girls. Parental supervision had a positive effect on children's privacy online – as parental supervision increased, the willingness to share personal data decreased and the likelihood of using privacy protection strategies increased. The protective effect, however, was observed in some areas more than others – children were disclosing less private information on dating suites and chat rooms, but still much more likely to do that on gaming platforms, social media and their own blogs.

Some of the behaviours that can be seen as risky (sharing passwords, pretending to be someone else online, posting personal information) can be explained by children's perception of the online environment as a place for socialising and the importance of sharing information for maintaining friendships (predominantly with people they already know). In most cases this information was shared with people they trust. In such cases parental supervision is not effective because it is incompatible with children's social needs and expectations. Trust in their social networks made children more likely to disclose personal information and less likely to engage in protective behaviours. The children who use the internet more engage more in communication with friends in building their social networks and are more likely to share more personal information and be less protective of their privacy. While effective in reducing privacy risk-taking, parental supervision cannot remove risks – even children with the highest level of parental supervision who were amongst the most active in social interaction were less likely to display privacy-protective behaviour than those with low levels of engagement in social interaction.

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

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 the notion of privacy conceptions – individuals' specific ideas of privacy – suggesting that differences in privacy concerns between the young and the old are due to the different developmental life stages; this is based on questionnaire data amongst adolescents (aged 12-19), young adults (aged 20-30) and adults (aged 31+). It uses Vedder's four dimensions: relational, spatial, decisional and informational.

The authors argue against the notion that young people are less concerned about privacy compared to older people. Instead, they hold that the 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?). They use a developmental perspective to underpin the study – adolescents' developmental goals are important for the articulation of the privacy conceptions. The authors argue that the focus of their privacy conception is their vulnerability to their parents' intrusions. The internet and social networking sites may be an opportunity to escape parents' scrutiny rather than being seen as a privacy risk.

The results show that young people do report less privacy concerns compared to older people, but adolescents associate relationships with privacy, unlike the group of young adults and that of adults over 31 years who are more likely to associate privacy with data collection, profiling, identity theft etc. The reported lower privacy concerns can be understood as part of development that is likely 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 the 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 a strong association of privacy with data collection concerns – the authors hypothesise that this is because adolescents are not yet the targets of banks, employers or government agencies; especially as this shifts for the young adults group.

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

Age: Adolescents (12-19 years), young adults (20-30 years) and adults (31 years and older) [categorised as 12-15, 16-19, 20-25]
Privacy type: Interpersonal
Data type: Given
Method: Survey
Country: USA
Study focus: Attitudes and behaviours
Platform: Social networking sites

The article explores how privacy conceptions and a risk–benefit trade-off mediate the effect between age, use of social networking sites and concern regarding privacy. Privacy concern is measured via four items (and a 4-point Likert scale): whether the participant is concerned about their privacy, think their privacy is important, feel they have too little privacy, or consider the internet as a threat to their privacy. Privacy conception is measured via questions related to relationships, personal information, personal space and autonomy.

The study found that the risk–benefit trade-off mediated the relationship between participation in social networking sites and concern about privacy, suggesting the benefits of social network participation outweigh the risks for those who participate in these online networks. The relationship between age and concern was mediated by privacy conceptions. There was a significant relationship between age and privacy conceptions, as well as between privacy conceptions and concerns regarding privacy. These differences, however, could not be explained by whether an individual uses social networking sites. The authors conclude that: 'the differences in concern regarding privacy between young and old may always have existed and are of a developmental nature. Social media may, therefore, have served to make these differences become more apparent, rather than having actually caused generational differences in concern between young and old' (Steijn et al., 2016: 12).

Young people's understanding of privacy is less focused on personal information than adults', and they are less concerned about risks related to data mining, bankers, future employers and authorities that seem distant and less relevant. Therefore, it is not surprising that they report less concern about privacy and are more active on social media, which provides both personal and social benefits (e.g. for identity development, social support and relationship formation).

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

Age: N/A, teenagers
Privacy type: Interpersonal
Data type: Given
Method: Focus groups and a survey
Country: Malaysia
Study focus: Behaviours
Platform: Social networking sites

Drawing on gratification theory, the authors argue that social networking sites offer children opportunities for entertainment, building social relationships and identity construction. While children identified a number of social networking site-associated risks, including some relating to privacy (e.g. identity theft, negative effects of posting personal information), their benefits outweighted the concerns.

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

Age: 6-18 [categorised as 4-7, 8-11, 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Participatory workshops
Country: Global: Argentina, Australia, Brazil, Colombia, Egypt, France, Ghana, Italy, Kenya, Malaysia, Nigeria, Philippines, Thailand, Trinidad and Tobago, Turkey, USA
Study focus: Media literacy, attitudes
Platform: General

Based on research with 148 children from 16 countries, the study explored children's views on their rights in the digital age. Children mostly understood privacy as the need to protect their personal information, and the key issues they discussed related to adjusting privacy settings, durability and replicability of online information, lack of control to what happens to information shared online and desire for independence from parental oversight.

83. Third, A., Bellerose, D., Diniz de Oliveira, J., Lala, G. and 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)*. Sydney, NSW: Western Sydney University. Available at: 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

The main messages give a strong overview of the report. 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 their responsibility to others. They tend to possess an understanding of and strategies for addressing risks encountered online. The report suggests that children's framings of the internet and digital technology echo mainstream conceptualisations and discourses that can limit their imaginations. Methodology: 490 children aged 10-18 from 26 countries participated in UNICEF country office workshops – distributed data gathering

(see RERights methodology at http://doi.org/10.4225/35/5a248c6b047e5). There was individual and group work to collect data in a participatory manner.

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

Age: 8-21 [categorised as 8-11, 12-15, 16-19]
Privacy type: Interpersonal, commercial
Data type: Given, traces
Method: Survey
Country: New Zealand
Study focus: Media literacy
Platform: General

Using a survey on internet usage and cybersecurity awareness among children and young people aged between 8 and 21, the study found that privacy awareness increases with age, but in relation to some privacy risks it remains considerably low, even for young adults. Knowledge of the word 'privacy' increases with age – 22% of the 8- to 12-year-olds knew the term compared to 65% of the 13- to 17-year-olds and 74% of the 18- to 21-year-olds. This is much lower than other cybersecurity terms such as 'antivirus' (67% of 8- to 12-year-olds, 87% of 13- to 17-year-olds and 95% of 18- to 21-year-olds) or 'security warnings' (respectively 56%, 78% and 69%). Younger children were also less aware of security software across all devices, and awareness of software for tablets and mobiles was overall lower than for desktops for all age groups (8-12 years: 48% desktop, 13% tablet, 9% mobile; 13-17 years: accordingly 72%, 29% and 12%; 18-21 years: 97%, 31% and 29%). The younger group had much less understanding of different privacy-related security issues, such as allowing apps to access their camera, contacts and personal information (name, address and mobile number). Only 2% of the 8- to 12-year-olds reported awareness compared to 18% of the 13- to 17-year-olds and 24% of the over-18s. Similarly, small proportions knew that installed apps can access information not required for its operation and may use this information for other purposes such as online advertisements: 1% of 8- to 12-year-olds, 15% of 13- to 17-year-olds and 26% of 18- to 21-year-olds.

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

Age: Mean age was 16.78 years [categorised as adolescents]
Privacy type: Interpersonal
Data type: Given
Method: Survey
Country: Belgium
Study focus: Attitudes, behaviours
Platform: Social networking sites

Young people use social media to achieve development goals, such as identity formation, forming and maintaining friendships and romantic relationships, but they share more than they did before, raising concerns about increasing risks such as reputational damage, cyberbullying and future impact on work

or study opportunities. The study uses the Prototype Willingness Model framework (PWM) developed by Gibbons and Gerrard (1995),[24] which examines the cognitive factors mediating the effects of the environment (e.g. familial, social) on adolescent risk behaviour. The model has two pathways – a reasoned pathway (decisions and behaviours are formed on the basis of deliberation and existing attitudes and norms) and a heuristic social reaction pathway (behaviours result from social situations that adolescents encounter) – and examines the sharing of personal information about peer relations on Facebook. The study found that almost half of the adolescents (49%) do not share personal information about peer relations online, and only 4% share such information regularly, with girls being more likely to share than boys. The self-disclosing behaviour is mostly influenced by their rational decision to share, weighing the possible benefits and costs, rather than a spontaneous relation to a specific situation. The willingness to share is most strongly predicted by attitudes towards self-disclosure, with older adolescents being more likely to follow their own subjective evaluations rather than social influence. Subjective norms of parents and friends (but not of teachers) also influence adolecents' intention to share personal information – those who think that their parents and friends would not disapprove tend to share more.

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

Age: 9-13 [categorised as 8-11, 12-15]
Privacy type: Commercial
Data type: Given, traces
Method: Experimental
Country: Netherlands
Study focus: Behaviours
Platform: Social networking sites

Children lack the skills to recognise subtle advertising formats, such as using personal data to target advertising on social media, which is seen as making them more susceptible to commercial content than adults. The study found that using personal information about interests and hobbies to select which advertising products to display were effective in creating positive brand attitudes and consequently increasing intentions. This effect was mediated by advert 'likes' – children who liked the ad were more likely to have a positive attitude and intend to buy the products. Adjustment of ad colour based on the child's preference, their perception of ad relevance and their awareness did not have direct effects. This can be explained by 'an affective process indicating low levels of cognitive elaboration' (van Reijmersdal et al., 2017: 408), suggesting that children process advertising differently from adults and in a non-critical manner.

87. Velki, T., Solic, K., Gorjanac, V., et al. (2017) Empirical study on the risky behavior and security awareness among secondary school pupils – Validation and preliminary results. In P. Biljanovic, M.

[24] Gibbons, F.X. and Gerrard, M. (1997) Health images and their effects on health behavior. In B.P. Bluunk and F.X. Gibbons (eds) *Health, coping, and well-being: Perspectives from social comparison theory*. Mahwah, NJ: Lawrence Erlbaum Associates, Inc., 63-94.

Koricic, K. Skala, et al. (eds) *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics*, 1280-4.

Age: 14-18 [categorised as 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Survey
Country: Croatia
Study focus: Behaviours
Platform: General

A survey of secondary school children revealed that 78% have given the password for the email they are currently using to somebody else, and 8% say that more than one other person knows the password. Six per cent say that more than one person knows their Facebook password. The study found no differences based on age and gender.

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

Age: 14-19 [categorised as 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Interviews and focus groups
Country: USA
Study focus: Behaviours
Platform: General

Exploring the privacy strategies of low-income and minority ethnic youth, the study found that young people want to control the context in which their information is shared and who has access to it. Yet they often have limited access to technology and experience more strongly the need to share devices that may disturb their privacy and create the need for constant negotiation: 'the boundaries of sharing and privacy are constantly renegotiated at the intersection of localized social norms, economic and social capital, and the technical affordances of particular platforms and devices' (Vickery, 2015: 282). This leads to a blurring as to what constitutes a private or shared device.

Furthermore, young people of colour and people from low-income backgrounds are subject to greater surveillance through different activities and obligations. In this context, the mobile phone can serve as a status symbol and as a gateway to greater independence and freedom, but some teens also chose to disconnect as a way of maintaining privacy and reversing typical power dynamics. Others split their online activities across different platforms in a fluid and disconnected manner, which was 'deliberate privacy strategy intended to resist the ways social media industries attempt to converge identities, practices, and audiences' (Vickery, 2015: 289). Different contextual norms of privacy underpinned the different platforms, and young people navigated away from the ones they felt more closely monitored. Young people of colour and people from low-income backgrounds also experienced the misinterpretation of their identities and communicative practices by majority peers, which created a

complicated need to navigate across cultural contexts and the feeling of a lack of privacy when these contexts collapsed.

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

Age: 14-19 [categorised as 12-15, 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Interviews, participant observations, ethnography
Country: USA
Study focus: Behaviours
Platform: General

Networked privacy means that we have some control over the information we intentionally share online, but have limited control over what is revealed about us by our social networks. Privacy should not be conceived as being about concealing information; it is imperative that privacy is understood in relation to 'agency, transparency, control, context and disclosure' (Vickery, 2017: 196), and in a way that acknowledges the public nature of online visibility, the power dynamics and the relations of privilege. There are multiple levels of publicness and privacy that operate in online social networks, and more public settings (e.g. public pages) can override individual and more restrictive privacy settings (e.g. making one's 'likes' on public pages visible to everyone), leaving a discrepancy between individual and platform (commercial) operationalisation of privacy. While all young peeople balance strategies for protection with opportunities for participation, some marginalised groups also feel the need for self-censorship and disconnection, which silences them further.

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

Age: 10-13 [categorised as 8-11, 12-15]
Privacy type: Interpersonal, commercial
Data type: Given, traces
Method: Survey and interviews
Country: USA
Study focus: Media literacy, behaviour
Platform: General

Children are oblivious about the long-term effects of their online activities, and under-estimate the value of their personal information in the long run. Hence, they might engage in riskier online behaviours, making themselves vulnerable. Students, parents and educators alike lack the understanding of third party gathering and use of personal information, and may fail to recognise the privacy risks of online educational activities (84% of children receive homework that requires them to access materials online). Parents struggle to monitor what children do online, and also find it hard to understand the privacy protocols to support children sufficiently in relation to this. Forty-five per cent of children use privacy settings, while 8% do not use any settings. A quarter do not know if their account is public or private and 20% say that they have public accounts. Children learn about websites

and applications most often from parents (46%), friends (43%), and less often from siblings (28%) and teachers (30%). They seek help mostly from friends (51%) and less from parents (31%), teachers (30%) or siblings (26%). While children turn most often to their parents with questions, this decreases with age. The study also found a ditital technology leap around the age of 12-13, when children start to use more devices and spend more time online.

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

Age: 12-18 [categorised as 12-15, 16-19]
Privacy type: Commercial
Data type: Given
Method: Survey
Country: Belgium
Study focus: Behaviour, attitudes
Platform: Social networking sites

There is a growth in child-targeting websites employing online advertising, raising concerns that while companies use adverts that appear entertaining and attention-grabbing, children lack the necessary consumer skills, which makes them more vulnerable to profiling. Assessing the willingness to disclose to marketing companies 14 different types of personal data (via a 4-point Likert scale), the study found that 73% of teens question why websites need their personal data and are concerned how this data might be used (69%). Most teens check the website's terms and conditions before disclosing any personal details (74%), and might deliberately provide false personal data (61% of teens). Still, a majority disclose profile information including gender (76%), real name (71%), age (68%), favourite shops (68%), brands (69%) or hobbies (66%), as well as contact information such as email address (17%) or phone number (23%). The study also found that children who were less concerned about their privacy were more likely to disclose their personal data (both contact and profile data), and there was no difference based on age. Those who saw more benefits from data disclosure were also more likely to share their information. Girls were found to be less willing than boys to disclose contact details but more willing to disclose profile data. Futhermore, the study found that no type of parental mediation influenced the children's willingness to share profile information. Active co-surfing and restrictive mediation had some effect (statistically small) on reducing disclosure of contact information. This is explained with the possible decrease in parents' roles as socialisation agents at this age and the possible increase of peer influence.

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

Age: 12-18 [categorised as 12-15, 16-19]
Privacy type: Commercial
Data type: Given
Method: Survey
Country: Belgium

Study focus: Behaviour, attitudes
Platform: Social networking sites

See Walrave and Wannes (2011) for a discussion of the findings. Based on the findings that privacy concerns reduce the sharing of personal education and that parental mediation has little influence on children's sharing behaviour, the authors argue in favour of educational and awareness-raising compaigns as a more suitable way of improving children's understanding of online privacy risks and the consequences of online data profiling.

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

Age: 7-12 [categorised as 4-7, 8-11, 12-15]
Privacy type: Interpersonal
Data type: Given
Method: Survey
Country: USA
Study focus: Behaviour
Platform: Social networking sites

Children as young as nine use social media (Facebook, Twitter and MySpace being the most popular), misrepresenting their age in order to register, arguably with the knowledge of their parents. By the age of 12 most children were on social media (89%). Of the children actively using social media, 82% knew that strangers can access some of their information. These children need a set of social media skills expanding beyond an awareness of potential dangers and including the management of privacy settings.

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

Age: 15-25 [categorised as 12-15, 16-19, 20-25]
Privacy type: Interpersonal
Data type: Given
Method: Interviews
Country: USA
Study focus: Attitudes, strategies
Platform: Social networking sites

The article explores how young people express their civic engagement and identity online. The study identified three main expression patterns: blended (expression of beliefs both offline and online), bounded (restricted offline expresion, focus on online) and differentiated (expression varies based on the platform). Withholding expression online was related to concerns about privacy, the reaction of their audiences and possible future implications of such online activity.

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

Age: 16-18 [categorised as 16-19]
Privacy type: Interpersonal
Data type: Given
Method: Analysis of social networking profiles
Country: USA
Study focus: Attitudes, behaviour
Platform: Social networking sites

The study analysed the content of 100 social media profiles created by young people aged 16-18 and the information they share (demographic characteristcs, posts and comments, images, discussion of family or school-related issues, social activities and peer interaction, risky behaviours, sexual content, personal and identity information). The study found that social media sites are popular arenas for socialising and identity exploration, and also for sharing information about a range of behaviours identified as risky, such as 'substance use, crime, promiscuity' (Williams and Merten, 2008: 280).

96. 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 existing privileges (perhaps this refers to more skilled parents?), and also leaves out the most vulnerable groups of children, such as foster children. The existing 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 escalated to a potentially harmful situation but foreclosing these risks limits 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 control (prioritising long-term consequences over short-term desires) and risk coping (addressing an encountered problem in a way that reduces harm, which is influenced by teens and parents' risk perception). The author analysed 75 commercially available mobile apps on Android Play, and found that the overwhelming majority of features (89%) within

these apps supported parental control (monitoring or restriction) rather than active mediation. In addition, many of the apps were 'extremely privacy invasive, providing parents granular access to monitor and restrict 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 experience them as restrictive and invasive. The way forward suggested by the author involves encouraging teens to self-regulate their behaviour; designing apps based on teens' needs; and safety features that do not compromise privacy (e.g. by giving parents access only to meta-level information and not the granular details).

97. 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., 302-16.

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 & American Life Project's Teens and Privacy Management Survey of 588 US-based teenagers (aged 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 and 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, automatic location sharing); and (2) privacy risk coping involving seeking advice or engaging in safety behaviours such as posting fake information, deleting content, blocking or deleting contacts or 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 strategies to adopt. Parents who were more concerned engaged more in privacy measures but the different strategies they use had a 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. Parental active mediation was linked to higher likelihood of disclosure of sensitive information and engagement in safety behaviour, meaning that children made more autonomous decisions and were encouraged to learn from mistakes. Children whose parents were more concerned about privacy also

showed higher levels of concern and were, in turn, more likely to seek advice and engage in safety behaviours. Children who engaged in one type of risky behaviour (e.g. sharing basic data) were also more likely to engage in others (sharing sensitive information). Teens associated only risky interventions with a higher privacy risk, which, in turn, was linked with advice-seeking and coping behaviours, while sensitive information was associated only with coping behaviours, and basic information was not linked to either perceptions of higher privacy risk or coping behaviour. Based on this, the authors suggest 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 and corrective behaviours, but also frequency of use of social networking sites and children's network complexity. Active mediation was found to be more empowering as children engaged with social networks more, experienced some risk but also engaged in coping behaviours. This was observed particularly strongly for the children of highly engaged parents who had high engagement and complex social networks, despite the restriction from direct parental intervention (it is unclear why children of counselling parents didn't do better than highly engaged parents, and 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.

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

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: behaviours

Platform: General

Using a nationally representative survey with 800 teenagers aged 12 to 17 (Teens and Privacy Management Survey conducted by the Pew Research Center's Internet & American Life Project between 26 July and 30 September 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 Westin, 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 or

parents) can lead to regret. Younger people are more likely to regret their posts (27% of those over 25 compared to 54% of under-25s have regretted their posts, according to Croteau, 2013,[25] 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, 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 a 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 email 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 less sensitive 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 less sensitive 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).

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

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 a consumer socialisation framework, the teens' understanding of consumer behaviour is seen as influenced by

[25] Croteau, M. (2013) A quarter of young people have Facebook or other social media postings they may later regret. July 24. Available at http://company.findlaw.com/presscenter/2013/a-quarter-of-young-people-have-facebook-or-other-social-mediapos.html

'socialisation agents' such as parents, peers, educators and 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, providing less personal information, and expecting negative consequences from information disclosure.

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 – rule making, 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 and school education, and wanted the right to be forgotten (name removal request). Rule-making and co-surfing led to support for government regulation. Rule-making and discussion were associated with support for education at school. The right to be forgotten was not associated with any parental mediation style.

100. 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 (aged 12-13) in the USA – an age group on the cusp of being protected by COPPA and not being protected by it. Sixty-one per cent of respondents were girls, 39% boys. The author uses Rogers' (1975, 1983)[26] protection motivation theory as a theoretical framework, and identifies the determinants of adolescents' privacy concern levels, and how that affects their privacy protection behaviours, particularly e-marketers' information-collection practices. Rogers' theory suggests that individuals' assessments of risks and benefits associated with risky behaviour plays a pivotal role in motivations to protect themselves from such

[26] Rogers, R.W. (1975) A protection motivation theory of fear appeals and attitude change. *Journal of Psychology* 91, 93-114; Rogers, R.W. (1983) Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J.R. Cacioppo and R.E. Petty (eds) *Social psychology: A sourcebook*. New York: Guilford Press, 153-76.

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, information disclosure benefits, privacy self-efficacy) affect levels of online privacy control, which results 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 and teachers), additional information (reading privacy statements) or avoid using certain sites requiring personal information. Young adolescents' concerns over online privacy are 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.

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

Age: 14-18 [categorised as 12-15, 16-19]
Privacy type: Interpersonal, commercial
Data type: Given, traces
Method: Survey
Country: USA
Study focus: Strategies, media literacy, attitudes
Platform: General

Focusing on e-commerce, this study uses survey data from 395 high school students in the USA to examine gender differences in relation to perceptions of privacy risks, level of concerns and protective behaviours. The existing literature, it is suggested, shows that women are more concerned about privacy threats and unwanted use of their emails and private information, but that data on gender differences in privacy strategies is inconclusive. In relation to privacy management strategies, teenage boys have been found to provide more fake information, while girls tend to seek more advice.

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

Age: 16-19 [categorised as 16-19]
Privacy type: Commercial

Data type: Profile
Method: Experimental
Country: Belgium
Study focus: Strategies, media literacy
Platform: Social networking sites

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).[27] 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).

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

Age: 7-9 [categorised as 4-7, 8-11]
Privacy type: Interpersonal
Data type: Given
Method: Quasi-experimental
Country: Canada
Study focus: Media literacy
Platform: eBooks

The study explores the effectiveness of an interactive eBook (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, and provides a digital trail via a storyline involving superheroes trying to maintain their secret identity on the internet after losing their privacy-related cyberpowers. Privacy proficiency tests were carried out (using Wilcoxon signed-rank tests) showing a significant improvement in the children's privacy knowledge and retention after one week.

104. 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

[27] Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004) Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15(4), 336-55. http://dx.doi.org/10.1287/isre.1040.003

Country: Canada
Study focus: Strategies, media literacy
Platform: eBooks

The article discusses the research summarised in Zhang-Kennedy and Chiasson (2016) with the addition of a control group where a text-only version was used while the treatment group used the eBook. The privacy proficiency test contained four knowledge-based questions and six scenario-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-only 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).

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

Age: unspecified [adolescents]
Privacy type: Interpersonal
Data type: Given
Method: Content analysis
Country: Germany
Study focus: Behaviour (practices)
Platform: Other social sites

The study analyses the content of the MTV website 'Over the Line' aimed at youth as a space for anonymous sharing of experiences of online hurtful behaviour. It is argued that children modify their mode of communication online, which goes beyond the technical specifications of the media and corresponds to their identity. An example of this is turning to a group of anonymous strangers to share experiences of hurtful behaviour – very sensitive and private information – in order to receive emotional support. This might supplement or even substitute traditional face-to-face social support and can be seen as transforming the process of socialisation. Communicating with strangers in this context carries trust and closeness – characteristics that are usually ascribed to relationships with family or friends. This also shifts privacy from traditionally shared in non-public circles to being shared in a public space – creating a new way of dealing with what is seen as public and private.

References

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

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

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

Ahn, J., Subramaniam, M., Fleischmann, K.R., et al. (2012) Youth identities as remixers in an online community of storytellers: attitudes, strategies, and values. *Proceedings of the American Society for Information Science and Technology* 49(1), 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(3), 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(5), 2645-64.

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

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

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

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

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

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

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

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

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

Chai, S., Bagchi-Sen, S., Morrell, C., et al. (2009) Internet and online information privacy: An exploratory study of preteens and early teens. *Ieee Transactions on Professional Communication* 52(2), 167-82.

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

Chi, Y., Jeng, W., Acker, A., et al. (2018) Affective, behavioral, and cognitive aspects of teen perspectives on personal data in social media: A model of youth data literacy. In: G.

Chowdhury, J. McLeod, V. Gillet, et al. (eds) *Transforming Digital Worlds. iConference 2018. Lecture Notes in Computer Science.* Cham, Switzerland: Springer, 442-52.
Children's Commissioner for England. (2017) Life in 'likes': Children's Commissioner report into social media use among 8-12 year olds. London: Children's Commissioner for England, 1-42.
Coleman, S., Pothong, K., Perez Vallejos, E., et al. (2017) The internet on our own terms: How children and young people deliberated about their digital rights. London: 5Rights, 1-68.
Cortesi, S., Haduong, P., Gasser, U., et al. (2014) Youth perspectives on tech in schools: From mobile devices to restrictions and monitoring. *Berkman Center Research Publication* 2014-3, 1-18.
Culver, S.H. and Grizzle, A. (2017) Survey on privacy in media and information literacy with youth perspectives. *UNESCO Series on Internet Freedom.* Paris, France: UNESCO, 1-125.
Davis, K. and James, C. (2013) Tweens' conceptions of privacy online: Implications for educators. *Learning, Media and Technology* 38(1), 4-25.
De Souza, Z. and Dick, G.N. (2009) Disclosure of information by children in social networking - not just a case of 'you show me yours and I'll show you mine'. *International Journal of Information Management* 29(4), 255-61.
Dennen, V.P., Rutledge, S.A., Bagdy, L.M., et al. (2017) Context collapse and student social media networks: Where life and high school collide. *Proceedings of the 8th International Conference on Social Media & Society* Toronto, Canada: Association for Computing Machinery, 1-5.
Dey, R., Ding, Y. and Ross, K.W. (2013) Profiling high-school students with Facebook: how online privacy laws can actually increase minors' risk. *Proceedings of the 2013 Conference on Internet Measurement.* Barcelona, Spain.
Emanuel, L. and Fraser, D.S. (2014) Exploring physical and digital identity with a teenage cohort. *IDC '14 Proceedings of the 2014 Conference on Interaction Design and Children.* New York: Association for Computing Machinery, 67-76.
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.
Garbett, A., Chatting, D., Wilkinson, G., et al. (2018) ThinkActive: designing for pseudonymous activity tracking in the classroom. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.* Montreal QC, Canada.
Gelman, S.A., Martinez, M., Davidson, N.S., et al. (2018) Developing digital privacy: Children's moral judgements concerning mobile GPS devices. *Child Development* 89(1), 17-26.
Ghosh, A.K., Badillo-Urquiola, K., Guha, S., et al. (2018) Safety vs. surveillance: what children have to say about mobile apps for parental control. *Conference on Human Factors in Computing Systems.* Montreal, Canada.
Heirman, W., Walrave, M. and Ponnet, K. (2013) Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking* 16(2), 81-7.
Hofstra, B., Corten, R. and van Tubergen, F. (2016) Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior* 60, 611-21.
Ji, Y., Wang, G.J., Zhang, Q., et al. (2014) Online social networking behaviors among Chinese younger and older adolescent: The influences of age, gender, personality, and attachment styles. *Computers in Human Behavior* 41, 393-402.
Jia, H.Y., Wisniewski, P., Xu, H., et al. (2015) Risk-taking as a learning process for shaping teen's online information privacy behaviors. *International Conference on Computer-Supported Cooperative Work and Social Computing.* Vancouver, Canada: ACM, 583-99.

Kumar, P., Naik, S.M., Devkar, U.R., et al. (2017) 'No telling passcodes out because they're private': Understanding children's mental models of privacy and security online. *Proceedings of the ACM on Human-Computer Interaction* 1 (CSCW), 1-21.
Lapenta, G.H. and Jørgensen, R.F. (2015) Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday* 20(3).
Livingstone, S. (2014) Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications. The European Journal of Communication Research* 39(3), 283–303.
Livingstone, S. and Haddon, L. (2009) *EU Kids Online: final report 2009*. Available at: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf.
Livingstone, S. and Sefton-Green, J. (2016) *The class.* New York: New York University Press.
Livingstone, S., Mascheroni, G. and Murru, M.F. (2011) Social networking among European children: new findings on privacy, identity and connection. *Hermes* 59, 89-98.
Livingstone, S., Haddon, L., Görzig, A., et al. (2010) *Risks and safety for children on the internet: the UK report: full findings from the EU Kids Online survey of UK 9-16 year olds and their parents*. Available at: www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20reports/UKReport.pdf.
Livingstone, S., Mascheroni, G., Ólafsson, K., et al. (2014) Children's online risks and opportunites: comparative findings from EU Kids Online and Net Children Go Mobile. London: London School of Economics and PoliIcal Science.
Machold, C., Judge, G., Mavrinac, A., et al. (2012) Social networking patterns/ hazards among irish teenagers. *Irish Medical Journal* 105(5), 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(24), 1-22.
Martin, F., Wang, C., Petty, T., et al. (2018) Middle school students' social media use. *Educational Technology & Society* 21(1), 213-24.
Marwick, A.E. and boyd, d. (2014) Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16(7), 1051-67.
McReynolds, E., Hubbard, S., Lau, T., et al. (2017) Toys that listen: a study of parents, children, and internet-connected toys. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.* Denver, CO, USA.
Micheti, A., Burkell, J. and Steeves, V. (2010) Fixing broken doors: strategies for drafting privacy policies young people can understand. *Bulletin of Science, Technology and Society* 30(2), 130-43.
Miyazaki, A., Stanaland, A. and Lwin, M. (2009) Self-regulatory safeguards and the online privacy of preteen children: implications for the advertising industry. *Journal of Advertising* 38(4), 79-91.
Moll, R., Pieschl, S. and Brornme, R. (2014) Competent or clueless? Users' knowledge and misconceptions about their online privacy management. *Computers in Human Behavior* 41, 212-9.
Moscardelli, D.M. and Divine, R. (2007) Adolescents' concern for privacy when using the internet: an empirical analysis of predictors and relationships with privacy-protecting behaviors. *Family & Consumer Sciences Research Journal* 35(3), 232-52.
Moser, C., Chen, T. and Schoenebeck, S.Y. (2017) Parents' and children's preferences about parents sharing about children on social media. *Human Factors in Computing Systems*, 5221-25.
Mullen, C. and Hamilton, N.F. (2016) Adolescents' response to parental Facebook friend requests: The comparative influence of privacy management, parent-child relational quality, attitude and peer influence. *Computers in Human Behavior* 60, 165-72.

Murumaa-Mengel, M. (2015) Drawing the threat: a study on perceptions of the online pervert among Estonian high school students. *Young* 23(1), 1-18.
Ofcom. (2017) Children and parents: media use and attitudes report. London: Ofcom. Available at: www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf.
Ogur, B., Yilmaz, R.M. and Göktas, Y. (2017) An examination of secondary school students' habits of using internet. *Pegem Egitim Ve Ogretim Dergisi* 7(3), 421-52.
Öncü, S. (2016) Facebook habits among adolescents: Impact of perceived social support and tablet computers. *Information Development* 32(5), 1457-70.
Oolo, E. and Siibak, A. (2013) Performing for one's imagined audience: Social steganography and other privacy strategies of Estonian teens on networked publics. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 7(1), article 7.
Pangrazio, L. and Selwyn, N. (2018) 'It's not like it's life or death or whatever': young people's understandings of social media data. *Social Media and Society* 4(3), 1-9.
Pradeep, P. and Sriram, S. (2016) The virtual world of social networking sites: Adolescent's use and experiences. *Psychology and Developing Societies* 28(1), 139-59.
Raynes-Goldie, K. and Allen, M. (2014) Gaming privacy: a Canadian case study of a children's co-created privacy literacy game. *Surveillance and Society* 12(3), 414-26.
Redden, S.M. and Way, A.K. (2017) 'Adults don't understand': exploring how teens use dialectical frameworks to navigate webs of tensions in online life. *Journal of Applied Communication Research* 45(1), 21-41.
Rimini, M., Howard, C. and Ghersengorin, A. (2016) Digital resilience: Empowering youth online. Practices for a safer internet use. A major survey targeting Australia, Japan, Indonesia, Korea and Taiwan. Brussels: ThinkYoung.
Rode, J.A. (2009) Digital parenting: Designing children's safety *BCS-HCI '09 Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology* Cambridge, UK: ACM Digital Library, 244-51.
S-O'Brien, L., Read, P., Woolcott, J., et al. (2011) Understanding privacy behaviors of Millennials within social networking sites. *Proceedings of the ASIST Annual Meeting* 48, 1-10.
Selwyn, N. and Pangrazio, L. (2018) Doing data differently? Developing personal data tactics and strategies amongst young mobile media users. *Big Data and Society* 5(1), 1-12.
Shade, L.R. and Singh, R. (2016) 'Honestly, we're not spying on kids': School surveillance of young people's social media. *Social Media and Society* 2(4), 1-12.
Shin, W. and Kang, H. (2016) Adolescents' privacy concerns and information disclosure online: the role of parents and the internet. *Computers in Human Behavior* 54, 114-23.
Shin, W., Huh, J. and Faber, R.J. (2012) Tweens' online privacy risks and the role of parental mediation. *Journal of Broadcasting & Electronic Media* 56(4), 632-49.
Steeves, V. and Regan, P. (2014) Young people online and the social value of privacy. *Journal of Information, Communication & Ethics in Society* 12(4), 298-313.
Steijn, W.M.P. and Vedder, A. (2015) Privacy under construction: a developmental perspective on privacy perception. *Science Technology & Human Values* 40(4), 615-37.
Steijn, W.M.P., Schouten, A.P. and Vedder, A.H. (2016) Why concern regarding privacy differs: The influence of age and (non-)participation on Facebook. *Cyberpsychology-Journal of Psychosocial Research on Cyberspace* 10(1), 1-12.
Subrahmanyam, K. and Greenfield, P.M. (2008) Online communication and adolescent relationships. *The Future of Children* 18(1), 119-46.
Third, A., Bellerose, D., Dawkins, U., et al. (2014) Children's rights in the digital age: a download from children around the world. Abbotsford, Vic.: Young and Well Cooperative Research Centre. .
Third, A., Bellerose, D., Diniz de Oliveira, J., et al. (2017) Young and online: children's perspectives on life in the digital age. *The State of the World's Children 2017 Companion Report.* Sydney: Western Sydney University. Available at:

www.westernsydney.edu.au/__data/assets/pdf_file/0006/1334805/Young_and_Online_Report.pdf.
Tirumala, S.S., Sarrafzadeh, A. and Pang, P. (2016) A survey on internet usage and cybersecurity awareness in students. *2016 14th Annual Conference on Privacy, Security and Trust (PST).* 223-8.
van Gool, E., van Ouytsel, J., Ponnet, K., et al. (2015) To share or not to share? Adolescents' self-disclosure about peer relationships on Facebook: An application of the Prototype Willingness Model. *Computers in Human Behavior* 44, 230-9.
van Reijmersdal, E.A., Rozendaal, E., Smink, N., et al. (2017) Processes and effects of targeted online advertising among children. *International Journal of Advertising* 36(3), 396-414.
Velki, T., Solic, K., Gorjanac, V., et al. (2017) Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics.*
Vickery, J.R. (2015) 'I don't have anything to hide, but…': the challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society* 18(3), 281-94.
Vickery, J.R. (2017) *Worried about the wrong things: youth, risk, and opportunity in the digital world.* Cambridge, MA: MIT Press.
Walrave, M. and Heirman, W. (2011) Cyberteens: balancing between self-disclosure and privacy concerns? *Conference Papers - International Communication Association*, 1-33.
Walrave, M. and Heirman, W. (2013) Adolescents, online marketing and privacy: predicting adolescents' willingness to disclose personal information for marketing purposes. *Children and Society* 27(6), 434-47.
Weeden, S., Cooke, B. and McVey, M. (2013) Underage children and social networking. *Journal of Research on Technology in Education* 45(3), 249-62.
Weinstein, E.C. (2014) The personal is political on social media: online civic expression patterns and pathways among civically engaged youth. *International Journal of Communication (19328036)* 8, 210-33.
Williams, A. and Merten, M. (2008) A review of online social networking profiles by adolescents: Implications for future research and intervention. *Adolescence* 43(170), 253-74.
Wisniewski, P. (2018) The privacy paradox of adolescent online safety: a matter of risk prevention or risk resilience? *IEEE Security and Privacy* 16(2), 86-90.
Wisniewski, P., Jia, H., Xu, H., et al. (2015) 'Preventative' vs. 'reactive': how parental mediation influences teens' social media privacy behaviors. Association for Computing Machinery, Inc, 302-16.
Xie, W.J. and Kang, C.Y. (2015) See you, see me: teenagers' self-disclosure and regret of posting on social network site. *Computers in Human Behavior* 52, 398-407.
Youn, S. (2008) Parental influence and teens' attitude toward online privacy protection. *The Journal of Consumer Affairs* 42(3), 362-88.
Youn, S. (2009) Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs* 43(3), 389-418.
Youn, S. and Hall, K. (2008) Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors. *Cyberpsychology and Behavior* 11(6), 763-5.
Zarouali, B., Ponnet, K., Walrave, M., et al. (2017) 'Do you like cookies?' Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior* 69, 157-65.
Zhang-Kennedy, L. and Chiasson, S. (2016) Teaching with an interactive e-book to improve children's online privacy knowledge. *Proceedings of the 15th International Conference on Interaction Design and Children.* Manchester, UK.

Zhang-Kennedy, L., Abdelaziz, Y. and Chiasson, S. (2017) Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction* 13, 10-8.

Zhang, Y. (2012) College students' uses and perceptions of social networking sites for health and wellness information. *Information Research-an International Electronic Journal* 17(3).

Zizek, B. (2017) Digital socialization? An exploratory sequential analysis of anonymous adolescent internet-social interaction. *Human Development* 60(5), 203-32.