Child Abuse & Neglect 117 (2021) 105064

Contents lists available at ScienceDirect

Child Abuse & Neglect

journal homepage: www.elsevier.com/locate/chiabuneg

# Teaching privacy: A flawed strategy for children's online safety

David Finkelhor *, Lisa Jones, Kimberly Mitchell

*Crimes against Children Research Center, University of New Hampshire, Durham, NH, 03824 USA*

ARTICLE INFO

*Keywords*
Online grooming
Cyberbullying
Hacking
Identity theft

ABSTRACT

Teaching young people about "privacy" has serious defects if the goal is to promote children's online safety. This commentary points out some the key problems to programs and educational modules with this privacy orientation. Privacy is an abstract and complicated concept, whose norms are in flux, making it difficult to impart clear, relevant, consensus-based messages. We also know very little about how privacy concepts develop in childhood and at what age and in what sequence, making it hard to know what to teach and when. Privacy skills are not necessarily the most important ones for preventing most online harms, including the most serious ones, casting doubt on whether they should receive priority over other prevention skills. Research has also not clearly established connections between many privacy practices and reductions in harm. Most privacy messaging has not been evaluated for how well it is learned, applied and what forms of safety it enhances. As an alternative, the promotion of online safety is best organized, not around privacy, but around the specific harms that educators and children themselves are trying to prevent. The highest priority of these are sexual exploitation, peer bullying and harassment. Such educational safety programs are best built from the foundation of evidence-based programs related to parallel offline dangers.

## 1. Introduction

Privacy has become a central concept in the public policy world struggling to manage the dangers thought to accompany the rapid growth of the digital environment (Auxier et al., 2019; Draper, 2019). So, it is not surprising that this concept has increasingly percolated into the discussion about dangers to children and the ways to keep them safe, particularly from sexual exploitation, bullying and harassment (Information Commissioner's Office, 2018; Lapenta & Jørgensen, 2015). Numerous articles have been published that focus on how to protect children's privacy (Allaert, Melina, & Sert, 2019; Johnson, 2018). Many educational programs have also been developed that put a strong emphasis on privacy skills primarily at the middle and high school level (International Computer Science Institute, n.d.; Office of the Privacy Commissioner of Canada, n.d.; Raynes-Goldie & Allen, 2014). (To reflect these middle and high school age targets, the term youth will be used.) Some of these programs refer to themselves as privacy education or teaching (Fordham University School of Law, 2021; International Computer Science Institute, n.d.), but others have large privacy labeled modules as part of programs described as digital citizenship or digital education (Berkman Klein Center, n.d.; Office of the Privacy Commissioner of Canada, n.d.).

The privacy labeled programs and modules cover topics like guarding personal information, recognizing that people may not be

* Corresponding author at: Crimes against Children Research Center, University of New Hampshire, 125 McConnell Hall, 15 Academic Way, Durham, NH, 03824, USA.

*E-mail addresses:* David.finkelhor@unh.edu (D. Finkelhor), Lisa.Jones@unh.edu (L. Jones), Kimberly.Mitchell@unh.edu (K. Mitchell).

https://doi.org/10.1016/j.chiabu.2021.105064
Received 22 July 2020; Received in revised form 25 March 2021; Accepted 31 March 2021

who they say they are, that being online leaves footprints, managing reputation, commercial manipulation and being aware that others may be observing or monitoring you. The explicit dangers flagged in these programs are identity theft, cyber-harassment, sexual predators, damage to reputation with employers or schools and others. Programs emphasizing privacy skills are sometimes being substituted for or merged with other youth safety programs and their strategies, making this issue salient for those concerned more generally about child protection.

However, this focus on privacy skills to keep youth safe may be misguided. Privacy is an abstract and complicated concept whose consideration does not necessarily address the key safety needs of youth or provide a good conceptual basis for education or action. This commentary tries to outline some of the main problems that it poses.

### *1.1. Complexity of privacy concept*

Privacy is not a simple idea nor is it easily embodied in a clear, agreed-upon set of guidelines, like rules about staying healthy (e.g., get exercise, eat fruits and vegetables). Even experts on the subject debate about what privacy is (Peter & Valkenburg, 2011; Petronio, 2002; Solove, 2015), but most agree that it is very context specific (Livingstone, Stoilova, & Nandagiri, 2019; Nissenbaum, 2011; Steeves & Regan, 2014). What information is safe or appropriate to share with a friend is very different from what someone would share with a teacher or an Internet service. Livingstone et al. (2019) divide privacy contexts into three categories: interpersonal, institutional and commercial. But even within these categories, privacy is still very specific to many individual contexts. What someone should or should want to share with parents is different from what one might want to share with peers, two different interpersonal contexts. The same goes for doctors vs. teachers, two institutional contexts. Privacy needs also vary considerably from person to person according to their personality or experience (Christofides, Muise, & Desmarais, 2009; Selwyn & Pangrazio, 2018). Some people are comfortable having acquaintances know about their ailments or their love life, while others are not. In addition to personal preferences, privacy norms are in flux and being innovated (Livingstone et al., 2019), especially in the digital realm, and vary across cultures (Soffer & Cohen, 2014), all of which makes it very hard to discern and teach meaningful, consistent messages that relate to a multiplicity of contexts.

### *1.2. Implicit harms referenced in privacy education*

Privacy is also confusing because what is generally being considered in privacy discussions is actually protection against an extremely varied, but often poorly specified, set of different harms to people's safety, reputation and interests (Shin, Huh, & Faber, 2012). These are the major harm contexts that lie behind most privacy discussions: 1) Strangers trying to sexually solicit or groom youth for sexual activity. 2) Receiving inappropriate sexual images. 3) Being bullied, threatened or harassed. 4) Having one's computer hacked, valuable software or money stolen. 5) Being manipulated by technology companies or commercial enterprises. 6) Being spied upon by law enforcement, school authorities or government agencies and thus made vulnerable to sanctions or discrimination (Shade & Singh, 2016). 7) Having one's reputation damaged in the eyes of family, friends, future employers or colleges (Xie & Kang, 2015).

It is crucial to note that the privacy practice implications of these harms depend on who the dangerous actors are in these contexts – strangers, technology companies, or school companions (Nissenbaum, 2011; Stoilova, Livingstone, & Nandagiri, 2019). The privacy implications are also very dependent on the dynamics of the harm –from cookies, or image capture, or someone obtaining your password. This makes it very difficult to generalize about appropriate privacy. Information management skills useful in one harm context may have little relevance to another context.

### *1.3. Lack of specificity or clear logic model*

Unfortunately, much privacy education discusses privacy in a generic way without connecting specific privacy rules or actions to the specific harms from particular actors. For example, some messages from the Teaching Privacy curriculum are, "There's no anonymity," "You are always leaving footprints," and "Someone could be listening" (Teaching Privacy, n.d.). Such messages leave learners unclear about what the harm actually is. But without the harm context, youth have a hard time understanding the purpose of the rule or its importance. They may make incorrect inferences. "Someone could be listening" could prompt youth to avoid parental surveillance, not an identity thief. To get someone motivated to use privacy protections and be thoughtful about their actions, they need to think through the dynamics of particular harms that can occur from particular online actors.

This need to connect privacy to specific harms is also particularly important in domains where privacy norms are poorly developed or in flux as with digital technology and when helping learners understand why privacy rules matter. "Don't share your password" doesn't necessarily have salience until someone learns that with your password someone might steal money from your bank account (Kumar et al., 2017). This connection to harms is particularly vague or underappreciated in some of the less familiar contexts such as in relation to commercial entities (Soffer & Cohen, 2014).

### *1.4. Ignorance or value difference*

Moreover, the differing degrees of privacy concern and adherence to privacy practices that people manifest are not simply about knowledge or ignorance. They can turn out to be differing judgments, broadly shared, about the frequency, nature and ratio of harms and benefits with regard to specific actors. Being tracked by a commercial entity is not seen as a privacy concern by those who are thinking about it primarily as a way that music companies expand their music tastes. Having conversations surveilled appears

differently to those concerned about the preventing terrorists vs. those who believe their own or others political opinions might draw unwanted attention. All this means that it is hard to craft general privacy messages relevant to many people and many contexts.

### 1.5. Uncertain connections between privacy and harm

Another problem is that for many harms the actual dynamics are not yet fully understood even by experts, especially in novel or evolving environments. For example, what are the most common dynamics through which youth receive inappropriate pictures? Is it through someone harvesting private personal information or through incautious web-surfing or through the recklessness of peers? Moreover, privacy concerns are sometimes prompted by extreme examples that ultimately are shown to be rare and not representative when studies are done. There are also disagreements about how risky various privacy-related Internet practices are. For example, are there risks from posting in a widely accessible place a child in a bathing suit or the name of their school? Some experts contend these motivate molesters or abductors. Others contend, based on research evidence, that this does not comport with how sex offenders typically find child victims (Wolak, Finkelhor, Mitchell, & Ybarra, 2008). So, fully understanding the harm context, including uncertainties, is the key element when privacy is being discussed. But because of complexities and unknowns, this is generally missing in modules about privacy.

Very importantly, when the harm context is accurately analyzed, it can reveal that privacy skills or privacy protections are not the main or most important way of managing the risks. To prevent online sexual exploitation, for example, the most important skills are to recognize inappropriate requests from someone else in an interaction (Finkelhor, 2020). Since much of the grooming and exploitation, even online, occurs at the hands of people a youth knows, not strangers, privacy rules like "don't post personal identifying information or identifiable pictures" or "don't text with strangers" may not be effective or only marginally effective in avoiding this harm. In fact, studies have not found that sharing information online to be associated with sexual solicitations (Wolak, Finkelhor, & Mitchell, 2008; Ybarra, Espelage, & Mitchell, 2007).

Similarly preventing inappropriate image exposure may primarily require an understanding about how to navigate around websites and what not to click on and why. Having blocking software may prevent some exposure for some youth, but not the majority (Wang, Zhao, & Shadbolt, 2019). Preventing manipulation by commercial companies on the Internet primarily involves good decision making and critical thinking about what products or services you do or don't need, not managing your cookies. Keeping cookies off your browser or your email address out of public view may in some instances reduce some risk. But the core protective skills are much broader and diverse, and often are missing in generic privacy discussions.

### 1.6. Developmental acquisition of privacy concepts

We know little about the childhood acquisition of privacy concepts or other protection skills, knowledge that is crucially important to devising effective education. The acquisition of privacy concepts or skills is not a topic that has been extensively addressed by developmental research (Livingstone, 2014). So it is hard to know when the foundations for these ideas are set, and at what age they can be grasped (Byrne, Kardefelt-Winther, Livingstone, & Stoilova, 2016; Chaudron, Di Gioia, & Gemo, 2018; Livingstone et al., 2019; Steijn & Vedder, 2015). As a result, despite much messaging, we know little about how to teach about privacy effectively.

Youth and adults may view privacy issues differently in reasonable ways from a developmental standpoint. Privacy education sometimes reflects concerns about moral and social values masquerading as safety issues. In every generation, adults, consciously or unconsciously, try to enforce their particular values about decorum, language and sexual behavior on the young. To the extent that youth intuit this, they may be resistant. There is also evidence that youth may not give the same priority as adults to concerns about keeping information from advertisers or social media platforms (Livingstone, Kirwil, Ponte, & Staksrud, 2014; Madden, Lenhart, Duggan, Cortesi, & Gasser, 2013). Even when made aware of adults' perceived concerns, they do not necessarily change their privacy behavior (Selwyn & Pangrazio, 2018). While some educators see resistance as underlining the need for more education, it could reflect reasonably different values about complicated issues. Unless connected to clearly established harms about which there is agreement, some privacy teachings will be resisted as old fogeyism.

### 1.7. Possible negative effects

Privacy teaching may also have some inadvertent negative effects. Such education can convey misconceptions about the nature of online dangers and their dynamics (Steeves & Regan, 2014). We know that people in general have an exaggerated sense of threat from strangers compared to the higher risk from intimates or acquaintances, a persistent misperception that bedevils crime prevention and safety messaging in general. Many of the generic privacy messages do have such an implicit prioritization of stranger danger. Messages like "don't give out personal information" tend to reinforce intuitions that the priority danger is strangers. To the extent that it misleads youth in regard to risk assessment, such messaging may undercut overall efforts to improve safety awareness and skills.

Another boomerang effect can result when youth conclude that educators and other adults are exaggerating risk. When they hear overbroad privacy prescriptions like "don't give out personal information" that target vague harms, are hard to implement and clash with other norms, youth may become insensitive or scornful of advice from that teacher or any other adult source (Wisniewski, 2018).

Privacy oriented teaching can also create a false sense of security. It may convey the mistaken confidence that harms have been sufficiently parried by privacy interventions, such as strong passwords or blocking software, when in fact these interventions are not the most important strategies to defend against harms.

### 1.8. Conclusions

These concerns lead to some suggestions for aligning elements of privacy teaching with real harm minimization.

1) Privacy education and data privacy skills should not be marketed as the key strategies to keep youth safe from some of the most salient online harms like sexual exploitation and bullying. Rather, education should focus on these specific harms and their contexts and address the various ways to increase awareness and improve risk management skills. Some of what are currently taught as privacy skills or protections – such as setting defaults in social media – are obviously relevant to these goals, but their discussion should occur in the larger context of avoiding specific harms, not on their own. These skills should be referred to as risk management or harm reduction skills rather than privacy skills.
2) Educational programs targeting Internet dangers should prioritize teaching about the dynamics of the risky situations and how to manage them, rather than emphasizing privacy rules. This can include information on the operation of scammers, sexual abusers, bullies, and manipulative advertisers. For each of these domains, the focus of education should be how to detect risk and avoid being targeted or victimized. Some privacy-labeled modules in educational curricula do emphasize particular risks (Berkman Klein Center, n.d.; Common Sense Media, n.d.). For example, some modules help students think more critically about their online "reputation" or how to avoid manipulation by digital marketers. But it may not be best practice to talk about these as "privacy skills, " since a large portion of the education pertinent to these harms is broader than privacy. Reputation is largely about how someone actualy behaves, not just what information they share about that behavior. Avoiding manipulation is about understanding hidden motives in people or companies, not just about deleting cookies or knowing how tracking works.
3) Privacy skills and practices taught to prevent harms need to be confirmed as efficacious via research or a strong evidence-informed logic model. Many privacy exhortations are connected only speculatively or anecdotally with harms (Jones, Mitchell, & Walsh, 2014; Jones, Mitchell, & Walsh, 2014). It is not clear that "don't give out your name or address" is a general rule that is understood, followed or that reliably prevents any form of childhood harm. Research needs to substantiate that privacy protections make a difference if they are to be key elements to prevention strategies.
4) Educational programs about Internet harms containing privacy skills would benefit from building on the foundation of programs designed to prevent of parallel offline harms. For example, online grooming risks should be taught as part of education about sexual assault, and online bullying should be combined with education about offline bullying. Online theft and hacking should be part of general safety education that covers property crime. The pedagogy of these programs about offline risks is much better developed and better evaluated and more likely to be successful (Finkelhor, 2020).
5) Educational programs containing privacy skills need to prioritize the risks they address, given limited curricular bandwidth. The most emphasis should be placed on bullying and sexual exploitation. These harms have been proven to be the most serious in their consequences for youth (Finkelhor, Shattuck, Turner, & Hamby, 2013). There is clear consensus about many of the norms that need to be learned and a large research base about the dynamics of these problems and the efficacy of the educational messages (Gaffney, Farrington, Espelage, & Ttofi, 2018; Gaffney, Farrington, & Ttofi, 2019; Walsh, Zwi, Woolfenden, & Shlonsky, 2015). Issues like commercial exploitation, non-sexual personal image exposure, and reputational management may be important, but these risks are currently not well understood when it comes to youth and the norms are in flux. Some of the concerns in this area may also be generationally specific.
6) There are likely some generic safety skills that cut across many of the risk domains, but these are not in the privacy realm. The generic skills shown by the research to reduce risk-taking and victimization are in the socio-emotional skills domain and include things like emotion management, decision-making, disengagement, help-seeking, and empathy. Research suggests that there are advantages when designing education for specific dangers to include some of these more generalized coping abilities (Durlak, Weissberg, Dymnicki, Taylor, & Schellinger, 2011).

The point of view being advanced in this commentary may appear to be somewhat at odds with an alternative widely held intuition about privacy. This is the assertion that privacy needs and norms are important above and beyond concerns about safety and harm and can and should be taught independently because of their inherent value. This assertion may be true and does need further consideration. One might argue that most people bridle at the thought of strangers walking around their homes or going their papers without permission, and they don't need to imagine a specific harm to want teach children to internalize those boundaries. But many if not most privacy concerns arise in the concept of specifically anticipated harms like crime victimization or social ostracism. This commentary is arguing that under conditions like the new digital world where privacy norms are not fully established or in flux and even culturally contested, it is important to tether our education and enforcement around real (not imagined) harms that we can point to and state clearly why they support certain privacy practices. Privacy education for its own sake may ultimately have its place, but it still needs a lot of work, and should not be promoted as an alternative to safety education by people whose primary goal is to protect children from harm.

The arrival of new technology has spawned many new anxieties and conversations, all vying for priority in the public and educational marketplace. We are still sorting through the merits of various concerns. It behooves us to be critical in our thinking and try to rely as much as possible on empirical evidence as we strive to make progress on keeping children and youth safe.

## Declaration of Competing Interest

The authors declare that there is no conflict of interest relating to this manuscript, nor any financial interests.

## References


Allaert, S., Melina, C.-B., & Sert, E. (2019). How to protect our kids' data and privacy. *Wired opinion*. https://www.wired.com/story/protect-kids-data/.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Berkman Klein Center. (n.d.). Privacy and reputation. https://dcrp.berkman.harvard.edu/theme/privacy-and-reputation.

Byrne, J., Kardefelt-Winther, D., Livingstone, S., & Stoilova, M. (2016). *Global kids online: Research synthesis 2015–2016*. UNICEF Office of Research Innocenti and London School of Economics and Political Science. http://globalkidsonline.net/synthesis-report/.

Chaudron, S., Di Gioia, R., & Gemo, M. (2018). *Young children (0–8) and digital technology, a qualitative study across Europe*. Publications office of European Union.

Christofides, E., Muise, A., & Desmarais, S. (2009). Jun). Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? *Cyberpsychology & Behavior : the Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society, 12*(3), 341–345. https://doi.org/10.1089/cpb.2008.0226

Common Sense Media. (n.d.). Digital citizenship curriculum: Interactive lessons and activities for all students. https://www.commonsense.org/education/digital-citizenship/curriculum?grades=3,4,5,6,7.

Draper, N. A. (2019). *The identity trade: Selling privacy and reputation online*. New York University Press.

Durlak, J. A., Weissberg, R. P., Dymnicki, A. B., Taylor, R. D., & Schellinger, K. B. (2011). The impact of enhancing students' social and emotional learning: A meta-analysis of school-based universal interventions. *Child Development, 82*(1), 405–432. https://doi.org/10.1111/j.1467-8624.2010.01564.x

Finkelhor, D. (2020). Youth internet safety education: The evidence base, 10/25/2019 *Trauma, Violence & Abuse*, 1–15. https://doi.org/10.1177/1524838020916257.

Finkelhor, D., Shattuck, A., Turner, H. A., & Hamby, S. L. (2013). Improving the adverse childhood experiences study scale. January *Archives of Pediatrics & Adolescent Medicine, 167*(1), 70–75. https://doi.org/10.1001/jamapediatrics.2013.420.

Fordham University School of Law. (2021). *Privacy education*. Fordham CLIP. https://www.fordham.edu/info/24071/privacy_education.

Gaffney, H., Farrington, D. P., Espelage, D. L., & Ttofi, M. M. (2018). Are cyberbullying intervention and prevention programs effective? A systematic and meta-analytical review, 2018/07/26/ *Aggression and Violent Behavior, 45*, 134–153. https://doi.org/10.1016/j.avb.2018.07.002.

Gaffney, H., Farrington, D. P., & Ttofi, M. M. (2019). Examining the effectiveness of school-bullying intervention programs globally: A meta-analysis. *International Journal of Bullying Prevention*. https://doi.org/10.17863/CAM.36367

Information Commissioner's Office. (2018). Children and the GDPR. *The general data protection regulation*. https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf.

International Computer Science Institute. (n.d.). Teaching privacy. University of California Berkeley. https://teachingprivacy.org/.

Johnson, S. (2018). The bargain at the heart of the kid internet. *The Atlantic(Family)*. https://www.theatlantic.com/family/archive/2018/04/child-data-privacy/557840/?gclid=Cj0KCQjwl4v4BRDaARIsAFjATPl8D7PlnvesJLZFbbspt0OFn9zg77JE_eD1am9A9g-AE0wriY5oasQaAjL3EALw_wcB.

Jones, L. M., Mitchell, K. J., & Walsh, W. A. (2014a). *A content analysis of youth internet safety programs: Are effective prevention strategies being used?* Crimes against Children Research Center (CCRC), University of New Hampshire.

Jones, L. M., Mitchell, K. J., & Walsh, W. A. (2014b). *A systematic review of effective youth prevention education: Implications for internet safety education*. Crimes against Children Research Center (CCRC), University of New Hampshire.

Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (2017). 'No telling passcodes out because they're private' understanding children's mental models of privacy and security online. *Proceedings of the ACM on Human-Computer Interaction, 1*(CSCW), 1–21.

Lapenta, G. H., & Jørgensen, R. F. (2015). Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday, 20*(3). https://doi.org/10.5210/fm.v20i3.5568

Livingstone, S. (2014). Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications, 39*(3), 283–303. https://doi.org/10.1515/commun-2014-0113

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014). In their own words: What bothers children online? *European Journal of Communication, 29*(3), 271–288. https://doi.org/10.1177/0267323114521045

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

Madden, M., Lenhart, A., Duggan, M., Cortesi, S., & Gasser, U. (2013). *Teens and technology 2013*. Pew Internet & American Life Project Washington, DC.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, the Journal of the American Academy of Arts and Sciences, 140*(4), 32–48.

Office of the Privacy Commissioner of Canada. (n.d.). Privacy and kids. https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/privacy-and-kids/.

Peter, J., & Valkenburg, P. M. (2011). Adolescents' online privacy: Toward a developmental perspective. In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 221–234). Springer.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Raynes-Goldie, K., & Allen, M. (2014). Gaming Privacy: A Canadian case study of a children's co-created privacy literacy game. *Surveillance & Society, 12*(3), 414–426.

Selwyn, N., & Pangrazio, L. (2018). Doing data differently? Developing personal data tactics and strategies amongst young mobile media users. *Big Data & Society, 5*(1), 1–12. https://doi.org/10.1177/2053951718765021

Shade, L. R., & Singh, R. (2016). "Honestly, we're not spying on kids": School surveillance of young people's social media. *Social Media + Society, 2*(4), 1–12. https://doi.org/10.1177/2056305116680005

Shin, W., Huh, J., & Faber, R. J. (2012). Tweens' online privacy risks and the role of parental mediation, 2012/10/01 *Journal of Broadcasting & Electronic Media, 56*(4), 632–649. https://doi.org/10.1080/08838151.2012.732135.

Soffer, T., & Cohen, A. (2014). Privacy perception of adolescents in a digital world. *Bulletin of Science, Technology & Society, 34*(5-6), 145–158. https://doi.org/10.1177/0270467615578408

Solove, D. J. (2015). The meaning and value of privacy. In B. Roessler, & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 71–82). Cambridge University Press.

Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information Communication and Ethics in Society, 12*(4), 298–313. https://doi.org/10.1108/JICES-01-2014-0004

Steijn, W. M., & Vedder, A. (2015). Privacy under construction: A developmental perspective on privacy perception. *Science, Technology & Human Values, 40*(4), 615–637. https://doi.org/10.1177/0162243915571167

Stoilova, M., Livingstone, S., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age: Research findings*. London School of Economics and Politacal Science.

Teaching Privacy. (n.d.). Ten pricipals for ontline privacy. https://teachingprivacy.org/.

Walsh, K., Zwi, K., Woolfenden, S., & Shlonsky, A. (2015). School-based education programmes for the prevention of child sexual abuse. April 16 *The Cochrane Library*, (4)https://doi.org/10.1002/14651858.CD004380.pub3. CD004380.

Wang, G., Zhao, J., & Shadbolt, N. (2019). Are children fully aware of online privacy risks and how can we improve their coping ability? *arXiv preprint arXiv: 1902.02635*.

Wisniewski, P. (2018). The privacy paradox of adolescent online safety: A matter of risk prevention or risk resilience? *IEEE Security & Privacy, 16*(2), 86–90. https://doi.org/10.1109/MSP.2018.1870874

Wolak, J., Finkelhor, D., & Mitchell, K. (2008). Is talking online to unknown people always risky? Distinguishing online interaction styles in a national sample of youth internet users. *CyberPsychology & Behavior, 11*(3), 340–343. https://doi.org/10.1089/cpb.2007.0044

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. (2008). Online' predators' and their victims: Myths, realities, and implications for prevention and treatment. *The American Psychologist, 63*(2), 111–128. https://doi.org/10.1037/0003-066x.63.2.111

Xie, W., & Kang, C. (2015). See you, see me: Teenagers' self-disclosure and regret of posting on social network site. *Computers in Human Behavior, 52*, 398–407. https://doi.org/10.1016/j.chb.2015.05.059

Ybarra, M. L., Espelage, D. L., & Mitchell, K. J. (2007). The co-occurrence of Internet harassment and unwanted sexual solicitation victimization and perpetration: Associations with psychosocial indicators. *Journal of Adolescent Health, 41*(6 Suppl 1), S31–S41. https://doi.org/10.1016/j.jadohealth.2007.09.010