Learning, Media and Technology
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/cjem20

Tweens' conceptions of privacy online: implications for educators

Katie Davis [a] & Carrie James [a]
[a] Graduate School of Education, Harvard University, Cambridge, MA, USA

Available online: 19 Mar 2012

To cite this article: Katie Davis & Carrie James (2012): Tweens' conceptions of privacy online: implications for educators, Learning, Media and Technology, DOI:10.1080/17439884.2012.658404

To link to this article: http://dx.doi.org/10.1080/17439884.2012.658404

Learning, Media and Technology
2012, 1–22, iFirst article

Tweens' conceptions of privacy online: implications for educators

Katie Davis* and Carrie James

Graduate School of Education, Harvard University, Cambridge, MA, USA

(*Received 24 October 2011; accepted 6 January 2012*)

There is considerable debate about young people's concern for privacy today, given their frequent use of social media to share information and other content about themselves and others. While researchers have investigated the online privacy practices of teens and emerging adults, relatively little is known about the attitudes and behaviors of younger youth. Drawing on interviews with 42 middle school students, or 'tweens', we explore how youth in this age group think about and manage privacy issues online, as well as the messages they report hearing from educators about online privacy. Our findings suggest that most tweens value privacy, seek privacy from both strangers and known others online, and use a variety of strategies to protect their privacy online. Further, tweens' online privacy concerns are considerably broader than the 'stranger danger' messages they report hearing from teachers. We discuss the educational implications of these findings.

Keywords: digital media; privacy; middle school students; Internet safety; citizenship curricula

Introduction

Marisa[1] is a 10-year-old Latina youth who enjoys participating in virtual worlds and using instant messenger and *Facebook* to socialize with her friends. As she engages in these activities, Marisa is keenly aware of risks – especially those related to privacy. When she goes online, she considers ways to protect her privacy from both strangers and friends. Although she is only 10 years old, Marisa's online privacy strategies are fairly sophisticated. She withholds sensitive, personal information from her *Facebook* profile and takes more proactive measures, such as using privacy settings and blocking unwanted contacts online. Marisa's strategies are informed by interactions with her parents, who give advice and oversee her online activities, and by her own practice of pausing and reflecting before posting content online. Her concerns about privacy are also informed by messages she has heard from teachers, which make her fearful of contact with strangers online.

*Corresponding author. Email: kdavis78@gmail.com

ISSN 1743-9884 print/ISSN 1743-9892 online

http://dx.doi.org/10.1080/17439884.2012.658404
http://www.tandfonline.com

In this paper, we draw on the voices of young people like Marisa in order to explore how youth think about and manage privacy issues online. Given the increasing use of the Internet and social media by children, tweens, and teens, privacy has emerged as an urgent topic of concern among parents, educators, and policymakers. A growing body of research suggests that while teens share a great deal online, their willingness to share does not mean that they care little for privacy. Less is known, however, about the attitudes and behaviors of younger youth and the role of educators in shaping these attitudes and behaviors. Such insight is needed in order to design effective educational interventions that are tied directly to early adolescents' distinct experiences with and understanding of online privacy.

The current study involved in-depth interviews with 42 'tweens', youth aged 10–14 years who were attending middle school at the time of their interview. We sought to understand the extent to which youth in this age group value privacy, the particular concerns they have about privacy online, the strategies they adopt to protect it, how they make decisions about what to share or withhold online, and the messages they hear from educators about privacy issues online.

Research context

Youth's attitudes toward online privacy

Recent studies of youth's digital media use confirm what parents and educators already know: young people share a considerable amount of information about themselves online. A 2006 survey of American teens (aged 12–17 years) found that 82% of teens with online profiles include their first name on their profile; 79% include photos of themselves; 61% include their city or town; and 49% include their school's name (Lenhart and Madden 2007). Since 2006, the amount of time that US teens spend online has increased (Lenhart 2011), and their information disclosure has followed suit (Lenhart et al. 2011; Thomas 2010). In addition, there is evidence to suggest that younger adolescents share more about themselves online than older adolescents; in their study of 12–18 year-old youth in Sydney, Australia, De Souza and Dick (2009) found that 12–14 year-olds disclosed more personal information on *MySpace* than 15–18 year-olds.

Young people's willingness to disclose information about themselves online is sometimes taken as proof that they do not care about their privacy (Marwick, Diaz, and Palfrey 2010). However, recent empirical evidence indicates that youth are both aware of and care about privacy risks online. A 2010 survey of 13–17 year-olds living in the USA found that 88% of teens said they worry about the consequences of posting their contact information online (Thomas 2010). Additionally, many respondents displayed awareness that what they post online may affect various aspects of their lives, such as their reputation, safety, and friendships, as well as their ability to get a job in the future and their chances of being admitted to the college of their choice. Younger adolescents and children are also concerned about their privacy

online (Devitt and Roker 2009; Lwin, Stanaland, and Miyazaki 2008; Steeves and Webster 2008; Youn 2009), with a majority believing that it is unsafe to post personal information online (Thomas 2008).

There appears to be a disconnect between youth's desire to protect their privacy online and their willingness to share personal information on sites like *Facebook*. In fact, existing evidence suggests that the two are uncorrelated (Christofides, Muise, and Desmarais 2009; De Souza and Dick 2009; Tufecki 2008). To explain this disjunction, Livingstone (2008)—whose research involves British teens—suggests that youth's conception of privacy online has less to do with the types of information they disclose and more to do with their desire to exert control over this information. According to Livingstone, '. . . teenagers must and do disclose personal information in order to sustain intimacy, but they wish to be in control of how they manage this disclosure' (2008, 405). Empirical evidence suggests that many young people living in Western societies feel they possess such control (Marwick, Diaz, and Palfrey 2010). This perception of control may help explain why youth are at once concerned about their privacy and willing to share their personal information online.

Social pressures are another likely cause of the disconnect between youth's concern about privacy and their online sharing habits. Social network sites like *Facebook* have become a central gathering place and mode of communication for young people (De Souza and Dick 2009; Debatin et al. 2009). Eighty percent of US teens with Internet access (Lenhart et al. 2011) and 82% of young adults use social network sites (Purcell 2011). A young person who chooses not to participate on these sites risks social isolation from his or her peers (boyd 2007; Tufecki 2008). For many youth in Western societies, the social rewards of sharing personal information online outweigh the perceived risks to their privacy (boyd and Marwick 2011).

The centrality of peers on social network sites may also illuminate an apparent disjunction between adults' and youth's online privacy concerns. While adults are primarily concerned with protecting young people from strangers online, the privacy concerns of North American youth extend to known others (Harris 2010; Steeves and Webster 2008). For both high school students and undergraduates, these known others tend to be adults, such as parents, teachers, and employers, although certain peers (e.g., acquaintances, romantic partners) may also be counted in this list (boyd and Marwick 2011; Marwick, Diaz, and Palfrey 2010; Thomas 2010; West, Lewis, and Currie 2009). Because they regard sites like *Facebook* as peer spaces, youth do not welcome the (increasingly large) presence of adults on these sites. In fact, many youth view their presence as an invasion of privacy (boyd and Marwick 2011).

Youth's privacy-protecting behaviors online

Adolescents and emerging adults employ a variety of strategies for protecting their privacy from both known and unknown others online. In fact, there is

evidence that young people's privacy-protecting behaviors on social network sites have increased over time to the point where they are more likely to engage in these behaviors than older adults (Marwick, Diaz, and Palfrey 2010; Young 2009). In their review of research on youth's online privacy practices, Marwick, Diaz, and Palfrey (2010) identified two broad categories of strategies employed by adolescents living in the USA, the UK, the European Union, and Canada. Avoidance strategies involve choosing not to use certain websites. Approach strategies include more proactive behaviors, such as providing false personal information, reading privacy statements, using privacy settings, and seeking advice from parents, teachers, or friends (Youn 2009). With respect to advice-seeking, a 2011 survey of 12–17 year-olds living in the USA found that fully 97% of respondents reported that they had received advice from at least one person about how to use the Internet safely and responsibly (Lenhart et al. 2011).

Providing false personal information emerged as the most popular privacy strategy among one sample of US high school students between the ages of 14 and 17 years (Moscardelli and Divine 2007). The popularity of this strategy seems only to have increased in the years since that study was conducted. A 2011 survey of US teens found that 49% of 12–13 year-olds and 42% of 14–17 year-olds admitted to falsifying their age online (Lenhart et al. 2011). As Marwick, Diaz, and Palfrey (2010) observe, these data suggest that youth's privacy-protecting behaviors, while perhaps more widespread than adults', may also be less ethical.

Drawing on interviews with US high school students, boyd and Marwick (2011) offer an alternate framework for understanding youth's privacy-protecting behaviors. Instead of avoidance and approach strategies, they distinguish between social and structural strategies for creating privacy online. With respect to social strategies, boyd and Marwick use the term 'social steganography' to describe youth's practice of hiding in public on social network sites like *Facebook*. This is done by using language and images that hold a particular meaning to a particular group of people. For instance, a young person might post lyrics to a song that played at a recent party or a quote from a movie that is popular among his or her close friends. Anyone who is not privy to these shared experiences, such as a parent, might infer an entirely different meaning from an exchange between friends than the friends themselves. In this way, youth embed hidden messages in the content they post publicly online.

Structural strategies involve making use of the technological affordances available on particular sites to control access to specific content (boyd and Marwick 2011). Examples of structural strategies include using privacy settings and creating restricted friend lists on social network sites. boyd and Marwick observe that this strategy is limited by the fact that youth do not always understand how to make use of technological affordances to protect their privacy online. This limitation may be particularly prominent among younger youth,

who tend to have a less sophisticated understanding of the technical and social complexity of the internet (Yan 2005, 2006).

Teaching online privacy

The research into youth's privacy attitudes and practices suggests a number of areas in which young people could benefit from educational supports. One such area includes education around the properties of networked publics that distinguish them from offline contexts and limit individuals' ability to exert full control over the information they share online (boyd 2007). An understanding of how easy it is to reproduce, spread, and search for information online, as well as how difficult it can be to delete information once it has been posted, may temper youth's confidence in their ability to retain control over what they share online. Other opportunities for intervention include educating youth about the use of privacy settings and engaging youth in conversations about the ethical implications of certain privacy-protecting behaviors like falsifying personal information online.

Over the course of the last decade, a variety of educational curricula have been developed in the USA that aim to promote young people's safe, responsible, and ethical behavior online. Examples include *i-SAFE*'s Internet Safety curriculum (http://www.isafe.org), *Common Sense Media*'s Digital Literacy and Citizenship curriculum (http://www.commonsensemedia.org/), and the educational materials produced by *Web Wise Kids* (http://www.webwisekids.org/). Some schools and school districts now mandate the use of such curricula as part of their educational technology initiatives. Indeed, in order to qualify for federal technology funds, the Protecting Children in the 21st Century Act requires schools to demonstrate that they have taken steps to educate students about appropriate online behavior. While the research into youth's privacy attitudes and practices suggests these efforts are well-placed, their effects on youth's online behavior remain unknown. It is not clear what messages youth take away from school-based initiatives, or whether these messages encompass the full range of privacy-related issues that youth confront online.

The current study

To date, most of the research on youth's online privacy attitudes and practices has involved high school and college students (e.g., boyd and Marwick 2011; Christofides, Muise, and Desmarais 2009; Lenhart and Madden 2007; Moscardelli and Divine 2007; Peluchette and Karl 2008; Robards 2010; Tufecki 2008; West, Lewis, and Currie 2009; Youn 2008; Young 2009). Relatively little is known about the attitudes and behaviors of younger youth, including the role of educators in shaping these attitudes and behaviors (Youn 2009). While tweens' technical understanding of the Internet is comparable to older adolescents, their understanding of the Internet's social complexity – including

online privacy – is somewhat less sophisticated (Yan 2005, 2006). This difference in understanding may give rise to distinct conceptions of and approaches to online privacy. In order to build effective educational interventions for middle school students around online privacy, it is important to understand how they think about these issues.

Moreover, the few studies that do involve tweens (e.g., Devitt and Roker 2009; Lwin, Stanaland, and Miyazaki 2008; Steeves and Webster 2008; Youn 2009) have not typically asked participants to reflect on the broad range of their privacy concerns, including their efforts to secure privacy from both known and unknown others. For instance, studies conducted by Lwin, Stanaland, and Miyazaki (2008) and Youn (2009) examined preteen and early adolescents' privacy practices in the context of e-marketing; these practices may differ markedly from those used to secure privacy from parents, teachers, or friends. The current study addresses this gap in the literature by drawing on interviews with 42 middle school students. It is guided by the following research questions:

Research Question 1: How do middle school students think about and manage privacy in new media environments?

Research Question 2: What messages do they receive from educators about online privacy?

Method

Sample

We recruited students from eight middle schools and one after school program in three school districts in the Greater Boston area. In order to obtain a diverse sample, we sought participants from six urban schools with racially and socioeconomically diverse students and from two suburban schools with largely white, upper-middle class students. The recruitment process involved two stages. First, we conducted surveys with a representative population at each school. Then, based on survey responses, we selected the most digitally engaged students to invite for interviews; we chose these students based on the assumption that their rich experiences would enhance their ability to reflect on the ethical issues and dilemmas with which we presented them. Students were contacted with an invitation to participate in interviews either by email or through a teacher at their school; parental consent was obtained before interviews were conducted.

Between February and August 2010, we conducted in-depth interviews with 42 youth between the ages of 10 and 14 years. The demographic characteristics of the sample are reported in Table 1. The online activities in which participants engaged included texting, talking on a cell phone, instant messaging, playing games, and the use of social network sites such as *Facebook* and, less often,

Table 1. Demographic characteristics of sample.

Age	
Range	10–14 years
Mean	12 years
Gender	
Female	24 participants
Male	18 participants
Grade in school	
5th grade	12
6th grade	11
7th grade	9
8th grade	10
Race	
Asian	4
Black	18
White	11
Other	9
Ethnicity	
African	4
East Asian	2
European-American	2
Latino	10
South Asian	2
Other	7
No response	15
Mother's education	
Less than high school	2
High school graduate or GED	7
Some college	6
College graduate	9
Graduate or professional degree	8
Don't know or did not report	10

MySpace. Many of our participants reported that they were under-aged users of social networks; researchers kept this information confidential, in accordance with human subjects requirements.

Data collection

Given our research goals – to understand how youth think about their online choices – we chose in-depth interviews as our principal method. In contrast to surveys, interviews allow for probing of participants' responses in order to capture rich details and nuances in their thinking and the subjective meaning

they grant to their activities (Weiss 1995). Our research team included five interviewers trained in qualitative methods. We conducted one-to-one interviews with participants in unoccupied classrooms and conference rooms either after school or during a study period. We interviewed each participant twice; on average, each interview lasted 45 minutes. By arranging two interviews, we ensured that we would have ample time to cover all of our questions without tiring participants or overly disrupting their schedules.

Because the current study is part of a broader investigation into the ethical dimensions of young people's online activities, our interview protocols included questions that extend beyond privacy, such as plagiarism, cyberbullying, and identity play. We asked different kinds of questions about these key topics in each of the two interviews conducted with each participant. We also posed general questions about participants' activities and choices online, and we asked them to respond to hypothetical scenarios. We used visual materials to facilitate our conversations with youth, such as colorful images depicting different new media activities and authentic mock-ups of social network profiles.

We asked participants a number of questions to elicit their conceptions of online privacy. We asked them to share their personal definitions of privacy; the strategies they use to create privacy online; the targets of their privacy strategies (i.e., the individuals from whom they seek privacy online); any experiences with privacy lapses online; and the messages heard from others (especially adults) about privacy online. We also raised privacy issues through the hypothetical scenarios. For example, we asked participants to respond to a mock social network profile in which a hypothetical friend was sharing emotions about family conflicts.

Data analysis

Interviews were digitally recorded and transcribed verbatim for coding and analysis. In addition, after each interview, researchers recorded notes about participants' responses to key questions, memorable anecdotes, and details about interview context and rapport. A team of five researchers developed the coding scheme, composed of both etic codes (derived from our research questions and the literature) and emic codes (themes which emerged from the stories and perspectives shared by our interview participants) (Glaser and Strauss 1967; Miles and Huberman 1994). Codes used in this analysis are described in Table 2. Codes were tied to specific interview questions; however, we also coded for unprompted comments. For example, in coding for 'online privacy strategies', we examined responses to one interview question, 'How do you create privacy online?' in addition to all other mentions of privacy-protecting behaviors. Findings from this code generated a subcode about how youth make decisions about which online privacy strategies to adopt.

Members of the research team obtained intercoder reliability through a multi-stage process that began with independently coding the same transcript

Table 2. Code descriptions.

Privacy definition	What does privacy mean to you?
Online privacy targets	Who do you want privacy from online?
Online privacy strategies	How do you create privacy online?
Online privacy lapses	Has someone ever not respected your privacy online?
Parent and teacher messages	Have you ever talked with anyone about privacy on the Internet? Have you ever talked with an adult? How about your parents? Has anyone spoken at your school about Internet safety or cyber-bullying? What did they say?

for a given set of codes. We then entered the coding into a qualitative software package (*N'Vivo*) and conducted a coding comparison test that produced the following statistics: Percentage of Agreement in the application of a given code; Kappa (a measure of agreement that takes chance into account); and Code Occurrence, or the percentage of each transcript in which the code was applied. We discussed any disagreements revealed by these tests and refined code definitions as needed. Following guidelines suggested by Landis and Koch (1977), we repeated this process until acceptable levels of Kappa (above 0.70) and Percentage of Agreement (above 0.80) were obtained; for the privacy codes, this process required two rounds of testing. We then divided and coded the transcripts independently. Reliability statistics for each code discussed in this paper are reported in Table 3. Given that we asked different questions in interview 1 and interview 2, we conducted separate reliability tests for each interview and reported results accordingly.

Findings

Findings from our study suggest that middle school-aged youth, or 'tweens', value privacy, seek privacy from both strangers and known others, and pursue various strategies to protect their privacy online. However, the messages they report hearing from educators focus on a rather narrow set of concerns. Below, we draw on the voices of our study participants to illustrate these findings.

Tweens' definitions of privacy

In order to elicit tweens' personal definitions of privacy – whether online or offline – we asked them, 'What does the word privacy mean to you?' Like Marisa, nearly all participants ($n = 41$, 98%) reported definitions that we would classify as 'conventional' – focused on maintaining control over their personal information and protecting it from unwanted audiences. For example, 10-year-old Gavin said privacy is '*... not putting too much information. Keeping yourself confidential and not showing too much of your*

Table 3. Reliability statistics, by code.

	Round 1			Round 2		
Node	Kappa	Agreement (%)	Code occurrence (%)	Kappa	Agreement (%)	Code occurrence (%)
Privacy, all codes (interview 1)	0.95	97.81	35.34	0.77	92.01	26.96
Privacy, all codes (interview 2)	0.68	86.70	36.02	0.74	89.33	33.90
Privacy definition (interview 1)	1	100	0.45	1	100	2.73
Privacy definition (interview 2)	1	100	0	1	100	0.00
Online privacy strategies (interview 1)	0.31	80.14	26.07	0.97	99.03	18.15
Online privacy strategies (interview 2)	0.71	93.81	15.08	0.77	94.13	18.17
Online privacy targets (interview 1)	0.51	90.18	16.00	0.79	94.50	18.32
Online privacy targets (interview 2)	0.37	92.00	10.62	0.76	94.94	14.18
Online privacy lapses (interview 1)	1	100	0.15	0.87	99.95	0.22
Online privacy lapses (interview 2)	1	100	0	1	100	0.00
Parent messages (interview 1)	0.74	91.84	23.38	0.99	99.73	11.68
Parent messages (interview 2)	0.70	90.61	23.95	0.91	96.09	34.32
Teacher messages (interview 1)	0.73	96.19	9.56	1	99.93	9.66
Teacher messages (interview 2)	0.80	95.55	14.98	0.84	95.73	18.49

identity online and stuff'. Gavin sees privacy as something to be protected or controlled by holding back information. Christina, age 11, spoke about privacy in terms of limiting audiences for her online content: '*just letting people that you know see it . . . like the things you put on your email or your Facebook or stuff like that*'.

Some tweens explicitly mentioned privacy invasions when discussing their definitions. For example, Zachary, age 12, talked about privacy as follows:

> I think of just being alone in the house or somewhere quiet. And online, to me, privacy is something like not a million people knowing who I am, not constantly

> trying to talk to me or bugging me or stuff like that. No viruses, no spyware, no key loggers, no Trojans, no stalking, stuff like that.

The privacy definitions shared by most tweens in our study suggest that they value this concept and would not subscribe to the famous statement made by Sun Microsystems' CEO Scott McNealy in 1999 that 'You have zero privacy, anyway. Get over it'. Only one tween suggested that privacy is not relevant or valued. Perry, age 14, said, '*I don't really think [privacy] means much anymore at this point. I mean, privacy to me is – most of my life is very public, and I know that*'.

Privacy targets

Tweens mentioned unwanted audiences for their online content at various points in the interviews. We also asked them the direct question, 'Who do you want privacy from when you're online?' Participants cited a range of targets. Perhaps not surprisingly, strangers ('people I don't know') were cited frequently, by 33 youth, or 79% of the sample. Emma, age 13, said she wanted privacy from:

> People who I don't know. Like people from other countries I don't really want looking at my profile. Like I'm fine with someone from [the] high school looking at mine, even though they didn't really know me. Like that's okay, because they live in the same town and I know a lot of – most people in this town are like good kids.

Emma differentiates between distant strangers ('people from other countries') and near strangers (high school students in her hometown). Terms like 'creepy people' and 'predators' were used by some youth when they mentioned distant strangers, which suggests a sense of fear about contact with unknown others online.

While fear of strangers was evident, participants were even more likely to cite wanting privacy from a 'known other'; 35 tweens, or 83% of the sample, cited at least one known individual. Marisa, described above, sought privacy from both friends and strangers. Similarly, when asked who she wants privacy from online, Makayla, age 12, said, '*Mostly friends. And mostly family members. Because if something happened, or I fell down, or a joke happened that is going to hurt me, or teasing, I'm going to be like, "Man, why did you put that up? I don't like that"*'. As suggested by Makayla, tweens' concerns often focused on the potential for the known others to share embarrassing information about them.

Looking more specifically at known targets, 30 tweens (71% of the sample) cited at least one known adult (a parent, teacher, other family member, and/or unspecified adults). Brianna, age 14, mentioned a specific event in explaining why she wanted privacy from adults at school: '*Like in school, yeah. Like one day, I was using my phone and [my teacher] took it from me, and they went through my texts to see who I was texting*'. Jonah, age 14, talked about

AIM, an instant messaging tool, as providing an important space for youth to vent with peers about adults online:

> Adults … Like on AIM, I just want it to be like a teenager world … Because sometimes you do talk about your teachers or your parents and how they're, what they're doing, and how it frustrates you and gets you mad and stuff.

Two-thirds of the sample (28 tweens, 67%) named other youth, such as friends, peers, siblings, and cousins, as privacy targets. Caleb, age 10, said '*My friends. I wouldn't know [sic] them to know specific things about me*'. Like many of our participants, Caleb suggests that there are certain things about himself that he withholds from even his friends. Other participants were explicit in placing their privacy concerns in the context of peer conflict – 'drama' – that they have observed and fear. Ashley, age 12, wants privacy from '*Just people … who like to start drama*'.

Related to this finding, we asked youth if they have ever felt that their own privacy was disrespected or invaded online. Only 10 participants (24%) reported an incident; notably, of these incidents, 7 (70%) were perpetrated by known others – for example, an adult or friend looking at participants' online content without permission, forwarding a text, IM, or FB message to unintended audiences, or sharing something about them that they had shared in confidence. Moreover, regardless of whether they personally experienced a privacy invasion online, many of our participants mentioned stories about friends or peers who had experienced invasions from known others.

Other specific targets mentioned less frequently by youth were institutions that can subject youth to surveillance (such as the police and the government) or individuals who can harm them (hackers, terrorists). One participant mentioned advertisers ('spammers') and one participant displayed awareness of future audiences when he cited future hockey coaches as targets from whom he wants privacy online.

Privacy management

Given tweens' conventional definitions of privacy and the range of target audiences they seek to avoid online, it is important to look at how they manage this complex landscape. We asked participants how they create privacy online and whether they felt it was 'hard' to do so. With respect to the latter question, nearly half of the sample (19 tweens, or 45%) responded that creating privacy online was *not* hard. However, another 19 participants said that they felt privacy was hard to create and 4 of these participants said that they 'can't' create privacy online or that they 'don't know how' to do it. One tween said that creating privacy online is just as difficult as creating it offline, and three tweens were not asked or did not respond to the question.

Despite the difficulties, some tweens reported with creating privacy online, all of our participants spoke about using privacy strategies, at least for certain

situations and contexts online, and most (36, or 86%) use a combination of strategies. Below, we describe two important dimensions of privacy management observed among the tweens in our study: the *strategies* they adopt – the things they do or don't do – in order to protect their privacy online, and the *processes* or factors that inform the strategies they choose. With respect to the former, our analysis revealed that participants employ withholding, proactive, or no privacy strategies. With respect to the latter, we identified three decision-making processes: interactions with others, reflection, and what we have termed the 'default' approach.

Privacy strategies

Withholding strategies. Mirroring the avoidance strategies identified by Marwick, Diaz, and Palfrey (2010), nearly all the participants in our study (40, or 95%) talked about strategies that involve withholding content from online spaces. Tweens talked about not posting certain personal information (such as their full names, addresses, and phone numbers) on their social network, instant messaging, or virtual world profiles. On *Facebook*, Ben, age 12, shares only his birth month and day, not the year, and his home state, but not the specific town in which he lives. Kevin, age 11, shares different kinds of information, depending on the platform he is using:

> Like for example, [on] Twitter, people could follow me any time they want to. So I just put a little bit of information and don't say that much. And like IM (instant messenger), I put a lot of, mostly a lot of my information, because it's just my friends and family, not other people, [on IM].

In talking about online privacy, some participants used the terms 'appropriate' and 'inappropriate' to refer to the kind of content they post or avoid posting online. Ahmed, age 12, asserted, '*I only put appropriate stuff. I don't talk about private things on MySpace*'. Examples of inappropriate content mentioned by tweens include naked pictures and comments containing swear words or sexual content. Lindsay, age 11, talked about withholding information that could be potentially embarrassing, '*I don't like giving information about me because I think it's going to be embarrassing, so I just keep it to myself*'.

Proactive strategies. Thirty-eight participants, 90% of the sample, spoke about using more 'proactive' measures to protect their privacy online. Adjustment of privacy settings on social networks to 'friends only' was the most prevalent proactive strategy, used by 27 participants. Fifteen participants (36%) spoke about embedding false information into their online profiles in order to protect their privacy. Notably, three of these youth shared that these deceptive privacy tactics were suggested by parents. Monitoring social network comments and photos in which one is 'tagged' – and deleting and 'untagging' as necessary – was another proactive strategy mentioned. Like many youth in

our sample, 13-year-old Kiara is friends with her mother on *Facebook*; she said that she untags herself from embarrassing baby pictures that her Mom posts.

Seven participants talked about more involved strategies for managing different audiences online and for creating more private spaces. Jade, age 14, actively maintains two *Facebook* accounts – one account that is open to her family and church friends, and one account for her school friends only. This strategy alleviates Jade's fears that her family and church circle will witness inappropriate online comments and photos posted by her school friends on *Facebook*. Another participant, Emily, age 12, talked about how she creates privacy on IM: '*On IM, I usually make a chat room with only the people that I want to tell, and I just tell them*'.

Absent strategies. While all participants in our study use withholding and/or proactive strategies at least some of the time, we observed that eight of these youth fail to employ privacy strategies on certain platforms or in certain situations online. Five of these tweens were unaware of privacy options on specific sites. For example, Tyler, age 12, uses proactive strategies (such as deception) to protect his privacy in a virtual world, but he was unaware of privacy settings on *Facebook*. Another participant, 13-year-old Danielle, chooses 'friends only' for photos when prompted by *Facebook* to choose who can see them; however, she was unaware of the general settings for her profile. Two participants reported awareness of privacy settings but had not bothered to adjust them, and one participant 'randomly' accepts friend requests in a game world.

Tweens' decision-making processes

Interactions with others. Thirty-three participants (79% of the sample) spoke about conferring with close relations when making decisions about how to manage their own and others' privacy online. Twenty-seven participants (64%) said that they confer with parents, and 16 (38%) reported talking with other youth (siblings or friends). Only one participant mentioned talking with a teacher. We classified such conversations as 'interactions' and observed both voluntary and involuntary forms. The majority of references to interactions (71%) appeared to be voluntary, 19% were involuntary, and the remaining references were unclear.

Voluntary cases included those in which tweens sought advice from parents or friends in relation to posting information or photos, adjusting privacy settings on social networks, and responding to friend requests from unknown people. Emma, age 13, spoke about turning to friends when she feels unsure about content she has posted online, '*Sometimes I'll just post some [information online] and if my friends will be – and then I'll ask my friends if it's okay and they'll either say, "Delete" or they'll say, "Yeah, it's fine"*'.

Six tweens (14%) spoke about checking in with friends before posting photos or comments about them online. These kinds of interactions were rarer in our sample, but are worth noting given the kinds of concerns tweens expressed

about privacy lapses by known others online. Impressively, three tweens talked about creating explicit guidelines with family or friends to respect each other's privacy online. For example, when asked how she creates privacy for her cell phone, 11-year-old Lindsay said, '*Me, my mom, and my sisters, we all agreed that nobody looks at nobody's phone, unless you tell them to*'.

Less voluntary interactions included parents monitoring participants' *Facebook* walls or watching over their shoulders as they communicate over instant messenger. When asked about her online interactions, 10-year-old Marisa said that she is careful about what she says and with whom she interacts '*because my mom watches the conversation*'.

We also examined the privacy strategies suggested by these interactions. We found that the majority of references to interactions (58%) suggested proactive privacy strategies, over a third (36%) suggested withholding strategies, and the remaining references did not indicate a specific privacy strategy.

Reflection. Twelve tweens, or 29% of the sample, told us that they take time to reflect on the potential consequences, for themselves or another person, of posting information or content online. The phrase, 'think before you post', was used by some tweens to capture the essence of this decision-making practice. Ben, age 12, articulated his approach by stating, '. . . *you just have to think before you put stuff up. Because when you put something on the Internet, it stays there . . . So anybody can always find you and stuff*'.

Ben's recognition that content persists online informs his reflective approach to making decisions about what he shares and, in this case, leads him to employ a withholding strategy. However, for other tweens, the relationship between reflection and privacy strategies is less clear; most participants spoke in generalities about using the process of reflection, but did not indicate the extent to which it led them to withholding or proactive strategies.

The default approach. Four tweens (10% of the sample) reported using what we call a 'default' approach to privacy choices online – they made a conscious choice to accept the default privacy settings on a given site based on the belief that the site designers considered privacy issues and built adequate privacy protections into the site's architecture. These tweens' comments suggest that their understandings were not always accurate. Anthony, age 11, said, '*You have to be friends to look at each others' information. I guess that's the rule on Facebook. It's [the] law*'. And Jose, age 12, said, '*Like in Twitter or on Facebook, you have to put where you live. And mostly, they only let you put Boston, Massachusetts, and that's it*'.

Educators' messages about online privacy

As discussed, a majority of tweens in our study cited use of 'interactive approaches', or conferring with adults or friends, to help guide their

decision-making online. We also asked participants several direct questions about the Internet-related topics that adults (educators and parents) have discussed with them.

Thirty-eight participants (90% of the sample) reported receiving messages about online privacy from an adult. Of these participants, 34 (89%) reported hearing messages from parents or other adult family members and 24 (63%) reported messages from educators. We were also interested in the substance of the messages heard from adults, especially educators. The most frequent messages tweens reported hearing from educators were '*Don't post personal information online*' (e.g., address, location, phone number) and '*Avoid interacting with strangers*'. Seventy-one percent of the participants who had received messages from educators said they heard a 'don't post' message, and 54% heard warnings about stranger interactions. Tweens reported hearing these two messages nearly as often from parents, although the top parent message was '*Don't post inappropriate content online*'.

One participant's account highlights how the 'don't post' and 'stranger danger' messages were often shared simultaneously by educators. Eleven-year-old Maya said,

> [My teacher] talked to us about it, and then when I got home I checked everything, just to make sure. I just got scared. Like I would go on Facebook and I'd check the account setting, and all that. I learned that not to share your personal things with people who you don't know, because they can just come to your house.

A response from another participant suggested that some educators use extreme scare tactics to get their messages across to youth. Marisa, age 10, said: '*[My computer lab teacher] said that people on the Internet, they can threaten you…they're going to hunt you and kill you. And that…they can find you and rape you*'.

Other messages heard from educators focused on data security (using strong passwords) (cited by four tweens); the importance of using privacy settings (four tweens); the public nature of the Internet and the persistence of content online (three tweens); and suggestions of safe websites (three tweens). Only one tween reported hearing a message from a teacher about respecting others' privacy online.

Discussion

To date, most of the research on youth's online privacy practices has involved high school and college students (e.g., boyd and Marwick 2011; Christofides, Muise, and Desmarais 2009; Lenhart and Madden 2007; Moscardelli and Divine 2007; Peluchette and Karl 2008; Robards 2010; Tufecki 2008; West, Lewis, and Currie 2009; Youn 2008; Young 2009). The current study investigated conceptions of and experiences with online privacy among a group of

younger adolescents between the ages of 10 and 14 years. Although age restrictions ostensibly prevent youth under the age of 13 years from accessing many websites, the reality is that youth in this age group are often frequent participants in online social networks and other spaces (Lenhart et al. 2011). Despite earlier research showing developmental differences in youth's understanding of the Internet's social complexity (Yan 2005, 2006), our findings revealed that tweens display many (though not all) of the same attitudes and behaviors around online privacy as older adolescents and emerging adults. Our findings also provide new insight into the decision-making processes that inform tweens' privacy strategies; the privacy-protecting messages that tweens hear from their teachers; the relationship between teachers' messages and tweens' privacy concerns; and opportunities for educational intervention around tweens' online privacy practices.

Consistent with research on high school and college students (Marwick, Diaz, and Palfrey 2010; Thomas 2010), the youth in our sample care about their privacy when they go online. They desire control over their personal information, and they want to feel they are protected from the attention of unwanted audiences, including people they know. Most participants displayed multiple privacy strategies, such as withholding information online and using privacy settings, and decision-making processes, such as conferring with close relations and reflecting independently on whether they should post certain content. These approaches appear to be influenced more by their peers and parents than by their teachers. Although participants did discuss hearing messages about privacy from teachers, these messages focused narrowly on stranger danger. In this section, we discuss these findings in light of existing literature and explore their educational implications.

Like older youth (e.g., boyd and Marwick 2011; Harris 2010), early adolescents desire privacy from known others in addition to strangers when they go online. In fact, the participants in our sample discussed wanting privacy from people they know more frequently than they discussed wanting privacy from strangers. They were more likely to identify adults than other youth, although fully two-thirds of our sample did say they sometimes want privacy from friends, acquaintances, siblings, or cousins. Participants were also more likely to talk about invasions of privacy involving people they know rather than strangers.

These findings suggest that, by focusing their privacy messages on strangers, teachers are not addressing the full range of youth's online privacy concerns. As boyd and Marwick (2011) found with the high school students they interviewed, the middle school students in our study regard sites like *Facebook* primarily as peer spaces. They may be 'friends' with their parents and other family members, but they do not want everything they post on *Facebook* to be viewed by these adults. In fact, they do not even want everything they share online to be viewed by all of their peers. By expanding their privacy discussions to include such concerns, teachers will be more aligned with what their

students are actually doing online. These discussions could help youth understand when it is and is not reasonable to expect privacy from certain people. Moreover, teachers could use these discussions to encourage their students to think about how their online actions affect other people's privacy.

Another area of opportunity for educational intervention concerns the strategies that youth employ to protect their privacy online. Over one-third of participants in our study said that they include false information about themselves to protect their privacy online. Although this is lower than the rate for older adolescents (13–17 years) (Thomas 2010), it nevertheless represents a sizable minority of youth. Disguising one's true identity is not uncommon online. Indeed, on many sites, including child-centered sites like *Habbo Hotel*, users are prohibited from providing their real names. However, there is a qualitative difference between presenting a username that is immediately recognized as such by others and creating a false identity intended to be taken at face value by certain people. The latter act suggests that it is acceptable to mislead other people in order to protect oneself. The ethics of such a stance are dubious. We believe it is an area around which teachers could engage their students in thoughtful conversations about the impact their actions have on other people and the communities in which they participate online. Such discussions represent a promising opportunity to promote students' digital citizenship.

Falsifying personal information was by no means the only strategy that the youth in our sample employed to protect their privacy online. Fully 86% of participants reported using multiple strategies that we categorized as either withholding or proactive strategies. These categories correspond to the avoidance and approach strategies discussed by Marwick, Diaz, and Palfrey (2010). Further, the most widespread proactive strategy in our sample, using privacy settings, corresponds to the structural strategies described by boyd and Marwick (2011). Notably, however, we did not find evidence that the early adolescents in our study engage in the practice of 'social steganography' that boyd and Marwick found to be popular among older youth. Two explanations for this discrepant finding strike us as plausible. First, it is possible that the participants we interviewed actually do engage in social steganography but they do not view these practices in privacy-related terms. Alternately, it may be that 'hiding in public' requires a level of sophistication that early adolescents do not yet possess. This second explanation aligns with Yan's (2005, 2006) research showing a positive connection between developmental maturity and young people's understanding of the social complexity of the Internet.

Developmental immaturity may also help explain why some of the youth in our study displayed ignorance or a lack of confidence about how to secure their privacy in certain situations. Without a sophisticated understanding of the privacy issues associated with online communication (an aspect of the Internet's social complexity), it is unlikely these youth would be aware of the range of measures they might take to protect their privacy. Further, although all participants spoke about using privacy strategies in certain circumstances,

our analyses revealed that there are several instances in which youth do not employ any strategies to protect their privacy online. There is opportunity here for teachers to develop their students' repertoire of privacy strategies and encourage them to think more broadly about when to use these strategies.

In addition to investigating youth's online privacy strategies, our study explored the decision-making processes they employ to arrive at these strategies. These processes include interactions with others, individual reflection, and what we call a 'default' approach that involves reliance on the privacy controls youth believe (correctly or not) to be built into a particular site. With respect to the individual reflection in which 12 youth (29%) said they engage, it is possible that teachers' privacy messages inform the nature of these reflections. Notably, however, only one youth included teachers in the list of people with whom she interacts around managing her privacy online. It is possible that teachers' focus on stranger danger messages discourages youth from approaching them about other types of privacy concerns. We are also mindful of the fact that many schools have restrictive policies around students' Internet use that may prevent teachers and students from engaging in conversations about online privacy. Both possibilities are regrettable, as our findings suggest there is need among early adolescents for education around online privacy management.

Limitations and future research

As with most qualitative research, our sample is small and was not drawn at random. Although we sought to create a sample that reflected the demographic characteristics of the region in which we conducted our research, we chose to include only youth who were particularly active digital media users. Therefore, we cannot claim that the findings are representative of all early adolescents in this region, and certainly not of the entire USA. It is possible that less-frequent digital media users approach issues of online privacy differently than the youth we interviewed. This possibility is supported by Yan's (2006) research showing that frequent Internet users tend to display a greater understanding of the Internet's social complexity. Thus, future research is needed to examine the online privacy conceptions and experiences of a broader range of early adolescents.

An important contribution of our study lies in its focus on a younger group of youth than has typically been included in research on young people's online privacy practices. We identified several consistencies between our findings and previous research involving high school and college students. At the same time, our findings suggest there may be some differences in the way tweens think about and approach online privacy; for example, we found no evidence that our participants engage in the practice of 'social steganography' that boyd and Marwick (2011) found to be popular among older youth. In future studies, researchers should explore in greater depth the possibility of developmental differences in youth's online privacy attitudes and behavior. For

instance, future research could investigate whether developmental maturity predicts individuals' familiarity with specific privacy-protecting measures. Moreover, because children's online experiences begin at increasingly young ages, these studies should include children who are even younger than the participants in our sample.

Lastly, although the interview method is well-aligned with our goal of understanding youth's perspectives on their digital media practices, we are aware of certain limitations associated with this method. Most notably, interviews elicit participants' descriptions of their behaviors rather than the behaviors themselves. These descriptions may be shaped by participants' desire to portray themselves in a favorable light, or by their imperfect memories. For instance, it is possible that some teachers' messages about online privacy are actually broader than warnings about strangers; such warnings may simply stand out in youth's memories. Although it is important to know that these messages are particularly salient to youth, future studies should seek to gather data from a wider range of sources, such as direct observations of class discussions about online privacy and interviews with teachers and parents about the messages they give to their students and children.

Conclusion

Over the last decade, online environments have become increasingly central in young people's lives. The present study offered insight into how a group of early adolescents navigate the privacy issues that arise in these new environments. Like older youth, the participants in our sample both care about and take measures to protect their privacy online. Yet, these measures are sometimes haphazardly employed and some youth display uncertainty or ignorance about how to protect their privacy. These findings suggest a need for educational intervention around online privacy targeted to the distinct experiences and attitudes of middle school students. At present, however, teachers' messages appear to be focused on a narrow – albeit important – range of youth's privacy concerns. Moreover, the privacy practices employed by the youth in our sample are shaped more by their parents and peers than by their teachers. We hope that the findings from our study will motivate teachers and school administrators to explore new ways of engaging with students around online privacy management.

Acknowledgements

The research reported in this article was funded by the John D. and Catherine T. MacArthur Foundation. The authors wish to thank the editors and referees of *Learning, Media and Technology* for their useful comments on earlier drafts of this article.

Note

1. All participants were assigned pseudonyms.

Notes on contributors

Katie Davis is a Project Manager at Harvard Project Zero. Her research focuses on the role of digital media technologies in adolescents' social, moral, and academic lives.

Carrie James is a Principal Investigator at Harvard Project Zero. Her research focuses on morality and ethics in new media environments, young people's engagement with digital media, and their participation in civic and political life.

References

boyd, danah. 2007. Why youth heart social network sites: The role of networked publics in teenage social life. In *Youth, identity, and digital media*. ed. David Buckingham, 119–42. Cambridge, MA: MIT Press.

boyd, danah, and Alice Marwick. 2011. Social privacy in networked publics: Teens' attitudes, practices, and strategies. Paper presented at the Oxford Internet Institute Decade in Internet Time Symposium, September 22, in Oxford, UK.

Christofides, E., A. Muise, and S. Desmarais. 2009. Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior* 12, no. 3: 341–5.

Debatin, Bernhard, Jennette P. Lovejoy, Ann-Kathrin Horn, and Brittany N. Hughes. 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* 15, no. 1: 83–108.

De Souza, Zaineb, and Geoffrey N. Dick. 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, no. 4: 255–61.

Devitt, Kerry, and Debi Roker. 2009. The role of mobile phones in family communication. *Children & Society* 23, no. 3: 189–202.

Glaser, Barney, and Anselm Strauss. 1967. *The discovery of grounded theory: Strategies for qualitative research*. Piscataway, NJ: Aldine Transaction.

Harris, Frances J. 2010. Teens and privacy: Myths and realities. *Knowledge Quest* 39: 74–9.

Landis, J. Richard, and Gary G. Koch. 1977. The measurement of observer agreement for categorical data. *Biometrics* 33, no. 1: 159–74.

Lenhart, Amanda. 2011. *'How do [they] even do that?' Myths and facts about the impact of technology on the lives of American teens* (Pew Internet & American Life Project). Presentation given at the Robert F. and Jean E. Holtz Center for Science and Technology Studies, Madison, WI. http://www.pewinternet.org/Presentations/2011/Apr/From-Texting-to-Twitter.aspx.

Lenhart, Amanda, and Mary Madden. 2007. *Teens, privacy, and online social networks* (PEW Internet & American Life Project). http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf.

Lenhart, Amanda, Mary Madden, Aaron Smith, Kristen Purcell, Kathryn Zickuhr, and Lee Rainie. 2011. *Teens, kindness and cruelty on social network sites: How American teens navigate the new world of 'digital citizenship'* (Pew Internet & American Life Project). http://www.pewinternet.org/~/media/Files/Reports/2011/PIP_Teens_Kindness_Cruelty_SNS_Report_Nov_2011_FINAL_110711.pdf.

Livingstone, Sonia. 2008. Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society* 10, no. 3: 393–411.

Lwin, May O., Andrea J.S. Stanaland, and Anthony D. Miyazaki. 2008. Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing* 84, no. 2: 205–17.

Marwick, Alice E., Diego M. Diaz, and John Palfrey. 2010. *Youth, privacy, and reputation: Literature review*. Cambridge, MA: The Berkman Center for Internet & Society, Harvard University, (Research Publication No. 2010-5) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163.

Miles, Matthew B., and A. Michael Huberman. 1994. *Qualitative data analysis: An expanded sourcebook.* Thousand Oaks: Sage Publications.

Moscardelli, D.M., and R. Divine. 2007. Adolescents' concern for privacy when using the internet: An empirical analysis of predictors and relationships with privacy-protecting behaviors. *Family and Consumer Sciences Research Journal* 35, no. 3: 232–52.

Peluchette, Joy, and Katherine Karl. 2008. Social networking profiles: An examination of student attitudes regarding use and appropriateness of content. *CyberPsychology & Behavior* 11, no. 1: 95–7.

Purcell, Kristen. 2011. *Trends in teen communication and social media use* (Pew Internet & American Life Project). Presentation given at Joint Girl Scout Research Institute/Pew Internet Webinar. http://www.pewinternet.org/Presentations/2011/Feb/PIP-Girl-Scout-Webinar.aspx.

Robards, Brady. 2010. Randoms in my bedroom: Negotiating privacy and unsolicited contact on social network sites. *PRism* 7, no. 3: 1–12.

Steeves, Valerie, and Cheryl Webster. 2008. Closing the barn door: The effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society* 28, no. 1: 4–19.

Thomas, Kim. 2008. *Tweens and internet safety*, *Cox Communications in partnership with the National Center for Missing & Exploited Children*. http://ww2.cox.com/wcm/en/aboutus/datasheet/takecharge/archives/2008-teen-survey.pdf?campcode=takecharge-archive-link_2008-survey_0511.

Thomas, Kim. 2010. *Teen online safety & digital reputation survey*, *Cox Communications in partnership with the National Center for Missing & Exploited Children*. http://multivu.prnewswire.com/player/44526-cox-teen-summit-internet-safety/docs/44526-Cox_Online_Safety_Digital_Reputation_Survey-FNL.pdf.

Tufecki, Zeynep. 2008. Can you see me now? Audience and disclosure regulation on online social network sites. *Bulletin of Science, Technology & Society* 28, no. 1: 20–36.

Weiss, Robert Stuart. 1995. *Learning from strangers: The art and method of qualitative interview studies*. New York, Toronto: Free Press.

West, Anne, Jane Lewis, and Peter Currie. 2009. Students' Facebook 'friends': Public and private spheres. *Journal of Youth Studies* 12, no. 6: 615–27.

Yan, Zheng. 2005. Age differences in children's understanding of the complexity of the internet. *Journal of Applied Developmental Psychology* 26, no. 4: 385–96.

Yan, Zheng. 2006. What influences children's and adolescents' understanding of the complexity of the internet? *Developmental Psychology* 42, no. 3: 418–28.

Youn, Seounmi. 2008. Parental influence and teens' attitude toward online privacy protection. *Journal of Consumer Affairs* 42, no. 3: 362–88.

Youn, Seounmi. 2009. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs* 43, no. 3: 389–418.

Young, Kirsty. 2009. Online social networking: An Australian perspective. *International Journal of Emerging Technologies and Society* 7, no. 1: 39–57.