Teen Privacy and Safety Online: Knowledge, Attitudes, and Practices

yth youth+ tech+health
Digital Trust Foundation
vodafone

Table of Contents

I. EXECUTIVE SUMMARY 3

II. BACKGROUND 8

Digital Privacy Project 8
Methodology 8
Participants 9

III. INTRODUCTION 10

IV. RESEARCH FINDINGS 14

Online Access 14
Social Media Preferences 15
Online Communication Practices 15
Online Information Sharing Practices 16
Online Privacy/Safety Concerns and Experiences 17
Online Privacy and Safety Attitudes 19
Online Privacy and Safety Practices 19
Peer to Peer Education 21
Knowledge, Attitudes & Behaviors Toward Online Privacy/Safety 22
Peer Advice on Management of Online Privacy/Safety 24

V. DISCUSSION 27

VI. RECOMMENDATIONS FOR ONLINE YOUTH PRIVACY COMPETITION AND CAMPAIGN 30

VII. APPENDICES 31

Appendix A. Focus Group Likes/ Dislikes of Popular Apps/Social Media Sites 31
Appendix B. Focus Group Online Information Sharing Practices 32
Appendix C. Actions Taken by Focus Group Participants to Protect Their Privacy 33
Appendix D. Examples of Peer Video Campaigns/Competitions 34

VIII. BIBLIOGRAPHY 37

I. EXECUTIVE SUMMARY

Today teens have tech-saturated lives. Threats to online personal safety and privacy are a growing risk that teens face as social media (i.e., social networking and messaging platforms) transforms the manner in which they interact and share personal information with each other. The concept of online privacy and safety is not static, but rather continues to evolve through advances in technology and with teens' increased use of the Internet, social media, and mobile apps. According to research from Pew, teens' actual technology use revolves around social media preferences, online communication, information sharing practices, experiences with online privacy and safety, and online privacy/safety attitudes and practices. Below are important findings from Pew Research Center's report on **Teens, Social Media, and Privacy (2013):**

- **Online Access** - Teens have robust levels of access to devices (i.e., desktop PC, laptop, tablet, phone, gaming consoles) for frequent and almost constant online access. Two-thirds of teens had access to more than one device. Smartphones and other mobile devices have become the primary devices for online access for teens.

- **Social Media Preferences** - Teens reported growing diversification in their social media preferences, and most used more than one social networking site. Although Facebook remains the social networking platform of choice for teens, younger teens—girls in particular—increasingly prefer visually oriented and anonymous sharing platforms.

- **Online Communication Practices** - Texting remains the primary mode of communication between teens. Although variations exist by gender, age, and race, teens are increasingly engaging with newer social media platforms that enable a broader range of communication modes. This allows for more diverse information sharing practices.

- **Online Information Sharing Practices** - The degree to which teens disclosed personal information—as well as the kinds of information they shared online—depended on the context. For example, teens disclosed a broad range of personal information for social benefit on social networking platforms, while on commercial websites teens disclosed both factual and false personal information in exchange for perceived benefits.

- **Online Privacy and Safety Experiences** - Many teens reported positive experiences online, however some experienced privacy breaches and encountered unwanted content and contact from others. Personal experience of privacy breaches can influence teens' online privacy behaviors, and individuals who experience unwanted contact are among

the most likely to say that they limit what other users can see on their profile.

- **Online Privacy and Safety Attitudes** - Teens cared more about threats to *social privacy* and less about personal data access by *corporate and government organizations*, and expressed high levels of confidence in their ability to self-manage. In the social context of information disclosure, younger teens are more likely to be concerned with potential risks to their physical safety, whereas older teens are more concerned with risks to their reputation.

- **Online Privacy and Safety Practices** - Few teens embraced a fully public approach in which they completely shared all information, and a large amount of effort is dedicated to managing privacy settings as well as engaging in reputation/network management practices (Marwick, Murgia-Diaz, & Palfrey, 2010). However, when teens are seeking advice—which is often in response to a crisis situation—they are more likely to turn to peers, friends, and family than go online for information or advice.

In understanding current teen attitudes and practices towards online privacy and safety, it is important to distinguish that teens care more about social privacy than they do about privacy in the context of third-parties and big data/information privacy. In comparison with earlier generations of teens, the modern vulnerabilities and risks to privacy and safety are heightened further by the persistent, visible, searchable, and spreadable nature of online social environments. A 2015 study cited that there are five top safety concerns with having youth online: harassment, solicitation, exposure, informational, and ethical risks (Wisniewski, Jia, Xu, Rosson, & Carroll). The privacy issue for many teens is now centered around the multiple facets of controlling a social situation, including Internet knowledge, having the power or agency within a social situation, understanding the social situation or context, and possessing the skills to manage the social situation. These skills are more valuable in current risks to online privacy than the technical aspects of digital privacy, which usually revolve around controlling information, access, or visibility. Within this context, teens' attitudes towards online privacy and safety are formed in the following ways:

- **Social media enables teens to extend and reinforce real-world peer relationships -** Posting information online is a way for youth to express themselves, connect with peers, increase their popularity, and bond with friends and peers. As a result, social media and mobile technologies play key roles in reinforcing both individual friendships and peer group relationships.

- **Teens' privacy norms vary according to the social context of their platform preferences** – Depending on the social media platform, young people want to be able to control what peers and non-peers are able to

view online within a social context. Teens aren't necessarily looking to "hide" from non-peers; rather, they define their restriction policies as a way to create privacy.

- **Teens tend to first disclose and then evaluate consequences** - The way teens learn how to manage privacy risk online is often very different from how adults approach privacy management. The process is more experiential in nature for teens, which is at odds with parental norms and values (Jia, Wisniewski, Xu, Rosson, & Carroll, 2015).

- **Teens' online practices appear risky to outsiders but are normative within a peer context** – Adults tend to project their norms and values onto teens without consideration for the teen experience. As a result, what adults interpret as a violation of "privacy" may actually be normative within a teen's peer context.

- **'Privacy' is a continuum along which teens adopt a 'risk-benefit' approach to sharing** - Although there is no founded correlation between providing personal data online and a lack of concern for privacy, choosing what to conceal or reveal is an intense and ongoing process for teens that involves trade-offs depending on the context.

- **Teens explore techniques to control interpretation of content to achieve privacy in public** - Limiting access to content by encoding hidden meaning within texts is a strategy that teens employ to control the social situation and reclaim agency.

- **Age and gender are key variables in understanding teens' privacy attitudes and behaviors** - As teens age, adult monitoring of activities begins to decline, and the likelihood of providing personal information online increases. While this makes teens more likely to hold increasingly sophisticated views of media literacy, it also leads to greater concerns over the potential for commercial misuse of their personal information. Girls are more likely to be concerned by privacy and feel more vulnerable to risks.

- **Teens' concerns and perceptions of risk—and their sense of vulnerability—influence privacy practices** - Teens are more likely to engage in a broad range of privacy-protecting behaviors, as well as manage privacy settings, if they are concerned with privacy, perceive information risk, or see themselves as vulnerable.

- **Researchers recommend active parental mediation over direct parental intervention** - Parents who use direct intervention may have a suppressive effect on teens, whereas a more consultative approach through active mediation may be more beneficial in protecting teens from severe online risks. Consultative approaches also empower teens,

leading them to engage with others online and learn to make good online privacy choices.

The networks that emerge as a result of the intersection of people, technology, and practice have significant implications for teens' privacy and safety online. Recognizing a teen's needs for privacy and autonomy within the social context is important for understanding their relationship to social media, as well as the privacy strategies that teens implement to counter the power dynamic that emerges through surveillance from adult authority figures. A key distinction that adults fail to make is that informational privacy is not as big an issue for teens as social privacy. This is not to say that informational privacy is not a valid concern, but that teens perceive it to be less of an intrusion on their privacy than surveillance by authority figures.

When participating in networks, teens tend to embrace a widespread "public-by-default, private-through-effort" mentality (boyd, 2014). Although research shows teens tend to rely on themselves to self-manage day-to-day privacy and employ considerable effort in managing privacy settings and other technical mechanisms of control, they often switch to a different medium such as messaging applications to communicate directly with peer audiences when they think information might be sensitive (Carroll & Kirkpatrick, 2011). When teens lack the resources to self-manage, they are more likely to seek advice on how to manage their privacy online from a friend, peer, or family member than an authority figure. Thus, peer education models are a powerful tool to influence behavior, knowledge, norms, and attitudes by providing spaces in which individuals learn from their peers. Multiple studies have proven the efficacy and usefulness of peer education (Stakic, Zielony, Bodiroza, Kimzeke, 2003; Shiner, 1999; Turner & Shepherd, 1999). Digital privacy and security—which can be viewed as sensitive subject matter among teens—may similarly benefit from peer models used for sexual health promotion and reproductive health (Bulduk & Erdogan, 2012; Alford, 2011a).

While parents, teachers, and other adults may not be the preferred go-to resources for information about Internet privacy, relying on peers for advice has a drawback—the quality of their advice may not necessarily match the rigor of information that could have been received from parents or other expert sources.

Proposed considerations for designing and implementing a digital privacy competition and campaign include:

- Interest categories based on teen demographics and privacy concerns (i.e., social privacy, mobile apps, security threats).

- Thematic categories based on standard control mechanisms (i.e., technical affordances), influencers (i.e., human, online), and innovative strategies (i.e., controlling meaning).

- Promotional outreach through preferred information (i.e., visually-oriented, humorous) and communication modes (i.e., short video format) and channels (i.e., Instagram, Vine, YouTube).

- Message concepts that appeal to the emotions of different teens (i.e., physical safety, digital reputation management, hacking) with verbiage that they use. Messaging that is empowering and not restrictive leads to creating a trusted environment. Approaches that are defensive and fear-based are often ineffective.

- Campaign resources need to be trustworthy, credible, easily accessible, and offer information in a nonthreatening way. Enhance search engine optimization (SEO) to improve search ranking and the promotion of digital privacy and safety websites.

- Endorsements from celebrities (i.e., Naya Rivera, Drake, Alex from Target, PewDiePie) and respected peer community leaders (i.e., digital literacy) to promote the competition and campaign.

- Popular culture events trigger heightened awareness and interest (i.e., bring risks to life, worst case scenarios) and monitoring for these will support timely promotional outreach.

Acknowledgements

YTH wishes to acknowledge the generous support of the Digital Trust Foundation and Vodafone Americas Foundation.

YTH also wishes to thank danah boyd and the Pew Research Center for their insights on youth online privacy and safety practices. Their contributions have informed much of the research outlined in this report.

II. BACKGROUND

Digital Privacy Project

YTH was awarded a grant from the Digital Trust Foundation in March of 2015. This grant focused on online privacy campaigns for youth. The proposed intervention aimed to use peer-to-peer education to increase positive attitudes and norms among teens around digital privacy practices and safe online behaviors. The project targeted teens between the ages of 13-17. Using a youth-centered participatory action approach, the project designed and implemented a national online campaign that used peer-generated video messages to increase knowledge and awareness of digital privacy and safety practices among young people. This national online campaign was also designed to promote behaviors that empower youth to protect their online privacy and safety through reinforcing positive digital privacy norms. Video testimonials tapped into peers' personal experiences and offered advice on how peers might effectively protect personal privacy and safety online. Because teens are in a better position to understand the concerns of their peers, this online campaign's use of peer-generated content is potentially more authentic and engaging.

Methodology

The formative research included a non-systematic review of publications and syndicated reports on current trends and issues regarding teen attitudes, knowledge, and behaviors. In addition, a review of evidence-based peer-to-peer education models—particularly those using digital media for disseminating messages designed to change behavior (Pew Research Center, published peer-reviewed journal articles and meta-analyses, and thematic books)—helped inform this research.

This study included four focus groups of 22 young people, ages 13 – 17, in Sacramento, CA. The four sessions were segmented by age and gender to help facilitate a conversation/discussion amongst peers.

The focus group discussions utilized open-ended interview questions in order to probe participants' use of technology for online access, online activities that they engage in, and their level of awareness, concerns, practices, and management related to online privacy and safety. Four separate focus groups were held in Sacramento, CA. Each group lasted approximately 90 minutes in length.

After a brief discussion of their online behaviors, the discussion focused on the following questions:

- Is privacy something that you are concerned with?
- How do you choose what to share online?

- What steps have you taken to protect your privacy online?
- Is there anything you find helpful/useful for managing online privacy?
- Where do you go for support if you have questions about online privacy?
- What advice around online privacy would you give to someone younger?

Participants

Below are the self-reported racial/ethnic identities of all participants, stratified by self-identified gender and age.

Race/Ethnicity	Female, Ages 13-14	Male, Ages 13-14	Female, Ages 15-17	Male, Ages 15-17
	Total (5)	Total (6)	Total (5)	Total (6)
African American	1		1	2
Caucasian	3	3	2	2
Hispanic/Latino		1	1	1
Asian		1		
Filipino		1		
Multiracial	1			1

III. INTRODUCTION

Teens' use of social media occurs simultaneously with their developing identity, emerging sexuality, physical development, and moral consciousness (boyd, 2014; Buckingham, 2008). Threats to online personal safety and privacy are growing risks that have evolved as social media transforms the manner in which teens interact and share personal information with each other. A 2015 study found that there are five top safety concerns with having youth online: harassment, solicitation, exposure, informational, and ethical risks (Wisniewski et al., 2015). The concept of online privacy and safety is not static and continues to evolve through advances in technology and with teens' evolving use of the Internet, social media, and mobile apps as an integral part of their social lives.

The most insightful research into understanding how teens conceptualize privacy and navigate social media is provided by researcher and author danah boyd (styled lowercase), who articulates an in-depth understanding of the mindset and underlying motivations for what teens are doing online and why. Her research frames the perspective of teens online, which helps adults understand the intersection between technology and youth culture and how this relationship influences teens' lives and practices. boyd's work moves beyond the lens of conventional research, which often frames the issue of teen Internet use from an outsider's perspective.

An important distinction that boyd makes in helping to understand teens' attitudes and practices towards online privacy and safety (and one that contrasts with adults' obsessive concerns and anxieties) is that teens care about social privacy more than they do about privacy in the context of third-parties and big data/information privacy. In comparison with earlier generations of teens, social media has increased the current generation of teens' access to social connection and autonomy via online networks (Biegler & boyd, 2010). boyd identifies **four defining characteristics that shape many of the mediated social environments created by social media:**

Persistence	The durability of online expressions and content (e.g., those using social media are often 'on the record' to an unprecedented degree)
Visibility	The potential audience who can bear witness (e.g., interactions are often public by default, private through effort)
Spreadability	The ease in which content can be shared (e.g., the ease with which people can share is unprecedented, which can be both powerful and problematic)
Searchability	The ability to find content (e.g., search tools are often designed to eliminate contextual cues such that content can often be taken out of context)

Research from boyd and others shows that teens care about their online privacy and safety. However, how teens understand and enact it may not immediately resonate or appear logical to adults. Because teens are more concerned about social privacy protection strategies that relate to friends and family, their concerns about organizational actors such as governments and corporations may seem irresponsible to adults. As a result, teens are trying to avoid surveillance from paternalistic adult figures in their lives such as parents, teachers, and other immediate authority figures. To teens, these individuals often use safety and protection as an excuse to monitor their everyday sociality. As a result, when teens seek privacy they do so in relation to those who hold power over them.

Teens' desire for privacy does not undermine their eagerness to participate in public. In boyd's view, there is a distinction between "in public" and "being public," such that teens want to gather in public environments to socialize but do not necessarily want their every posting to be publicized (2014). The privacy issue for many teens is more a matter of social norms and etiquette than managing technical aspects to control information, access, or visibility. Privacy is something they are actively and continuously trying to achieve through controlling a social situation using a combination of having power or agency within a social situation, understanding of the social situation and

context, and possessing the skills to manage the social situation in order to both understand and affect how information flows and is interpreted.

Achieving privacy requires the ability of individuals to control the social situation by navigating complex contextual cues, technical affordances, and social dynamics. When teens try to achieve privacy in networks they often struggle with these foundational elements. Controlling a social situation in an effort to achieve privacy is neither easy nor obvious. Because social situations are never static and often carry complex dynamics, the technical affordances for managing access and control change regularly such that maintaining skills can be overwhelming and require considerable effort. Teens respond to these limitations by working around technical affordances, reclaiming agency, and using novel strategies to reconfigure and control the social situation by controlling access to *meaning* rather than *content*. By doing so they seek to reclaim agency.

Educating teens about online privacy may benefit from a peer-to-peer education approach, rather than a top-down dissemination of information from adult to youth. Extensive research published in the last two and a half decades has shown that peer-to-peer education is a powerful tool to influence behavior, knowledge, norms, and attitudes (Jackson & Barnes, 2013; Bulduk & Erdogan, 2012; Alford, 2011b; Poland, Tupker, & Breland, 2002).

Peer education models vary broadly in settings, methods, and goals, as well as in the definition itself. In general, peer education is a strategy where individuals from a target population encourage or discourage behavior, knowledge, norms, and attitudes to their peers (Stakic et al., 2003; Turner & Shepherd, 1999).

Peer education can occur in a variety of settings including schools, universities, colleges, youth centers, social settings, outreach settings, work sites, and informal networks. More recently, peer education can occur online through education networks, massive open online courses (MOOC), online games, social media, and more (Beheshti, 2012). Peer education methods vary considerably and are often part of a multi-pronged strategy. Methods can include tutoring, one-on-one counseling or discussions, and facilitating group discussions. Peer education goals can include relaying information, behavioral change, knowledge acquisition, skills development, or community development.

The rationale behind peer education has been cited across the literature and in multiple meta-analyses looking at the effectiveness of peer-to-peer learning:

Peers are a credible source of information.

Peer groups can have many similarities. Such similarities allow peers to accept each other's viewpoints. Because teens often identify with their peers, presenting messages through these peer networks can increase the effectiveness of an education program's goal.

Peers can reinforce learning through ongoing contact.

As teens spend a great deal of time socializing and interacting with one another, in person and online, they have many opportunities to influence each other. A particular message or behavior can be reinforced often between peers.

Peer education can be used to access hard-to-reach populations.

Conventional education methods may not reach all individuals. Peer-to-peer models can convey culturally appropriate information, engaging hard-to-reach populations.

Peer education can communicate information in a youth-friendly style.

Using youth-friendly communication can help convey information in a more accepting way and in natural settings where target groups are located.

IV. RESEARCH FINDINGS

This section provides the foundation for understanding teens' actual technology use, social media preferences, online communication, information sharing practices, and practices/experiences with online privacy and safety. Additional evidence and information is compiled here based on a review of studies conducted by Pew Research Center on teens, technology, and privacy, published peer-reviewed journal articles and meta-analyses, thematic books, and focus group findings. This section also describes the rationale for peer-to-peer education, highlighting results from meta-analysis studies illustrating how peer education is effective in influencing behavior, knowledge, norms, and attitudes.

Online Access

Teens have robust levels of access to devices (i.e., phone, desktop, laptop, tablet, gaming consoles) for frequent and almost constant online access, with two-thirds having access to more than one device. Smartphones and other mobile devices have become the primary devices for online access for teens (Madden, Lenhart, Duggan, Cortesi, & Gasser, 2013). Our own focus groups findings corroborated Pew Research Center studies:

- **Mobile devices facilitate convenient and frequent online access** – Aided by the convenience and constant access provided by mobile phones, 92% of teens report going online daily, with 24% using the Internet "almost constantly" and 56% going online several times a day. Smartphone users are more likely to be older teens with 76% of 15- to 17-year-olds having a smartphone, compared with 68% of 13- to 14-year-olds. African-American teens are the most likely to have or have access to a smartphone (85%).

- A significant proportion of teens report "almost constant" Internet use – A majority (92%) of teens go online daily, and one-quarter (24%) go online "almost constantly." Among African-American teens, 34% report going online "almost constantly" compared with 32% of Hispanic teens and 19% of white teens. Youth from affluent families go online more frequently than youth from the least wealthy households; nearly all (93%) teens from homes earning more than $30,000 annually go online daily, compared with 86% of those from households earning $30,000 or less.

Social Media Preferences

Teens report growing diversification in their social media preferences. Although Facebook remains the social networking platform of choice for teens, younger teens—girls in particular—increasingly prefer visually oriented and anonymous sharing platforms. See Appendix A for focus group participants' likes and dislikes of popular social media sites.

Facebook remains the most popular social media platform among teens, but is becoming increasingly utilized by older individuals and parents. The site used most frequently by teens is Facebook (41%), followed by Instagram (20%), Snapchat (11%), and Twitter (6%). With growing diversification in social networking platform preferences, a majority (71%) reported that they use more than one social network site. Overall, the most popular choices are Facebook (71%), Instagram (52%), Snapchat (41%), and Twitter (33%). Focus group participants stated that older individuals, parents, and family are increasingly using Facebook. Male participants, ages 15-17, stated that they think about what they post on Facebook as if their grandmother would see it.

"My friends call Facebook 'Momsbook'."

-Focus Group Participant, Female, 13-14

Social media platform preferences vary by gender and age. Boys were found to visit Facebook more often than girls (45% vs. 36%), and girls were more likely use Instagram (23% vs. 17%) and Tumblr (6% vs. 1%). Older teens (15 to 17) were more likely to use Facebook (44% vs. 35%), Snapchat (13% vs. 8%) and Twitter (8% vs. 3%), while younger teens (13 to 14) were more likely to visit Instagram (25% vs. 17%).

Online Communication Practices

Texting remains the primary mode of communication between teens. Although variations exist by gender, age, and race, teens are increasingly engaging with newer social media platforms that enable a broader range of communication modes and allow for more diverse information sharing practices.

Social media platforms support a shift in teens' communication and information behaviors. A majority of teens (90%) with phones exchanged texts and 33% had messaging apps (i.e., Kik, WhatsApp). Some 47% of teens talk with others over video connections (Skype, Oovoo, Facetime and Omegle).

Anonymous sharing apps (Whisper, Yik Yak and Ask.FM) are used by 11% of teens with cell phones and more often by girls (13% versus 8%).

"I follow Nike [on Instagram] so I can see cool pictures of football cleats or something. If I like a girl, it's the 2015 version of flirting to 'like' someone's photo."

-Focus Group Participant, Male, 15-17

Girls use visually oriented social media platforms for sharing content more than boys. Teenage girls use Instagram (61% vs. 44%), Snapchat (51% vs. 31%), online pinboards like Pinterest and Polyvore (33% vs. 11%), as well as Tumblr (23% vs. 5%) and Vine (27% vs. 20%) for sharing more than boys do. Boys are more likely to have or have access to a game console (91% vs. 70%) and play video games online or on their phone (84% vs. 59%). One-in-six teens (17%) read or comment on online discussion boards like Reddit or Digg.

Online Information Sharing Practices

The degree to which teens disclose personal information as well as the kinds of information they share online depends on the context. For example, on social networking platforms teens disclose a broad range of personal information for social benefit, while on commercial websites teens disclose both factual and false personal information in exchange for perceived benefits. See Appendix B for focus group participants' online information sharing practices.

Teens disclose a broad range of personal information through online social networks. Teens are more likely to share real names (92%), photos of themselves (91%), interests (84%), birth date (82%), and school name and city/town where they live (71%) through social media platforms. Teens are less likely to post a cell phone number (20%), email address (53%), or a video of themselves (24%). Older teens (14-17) are more likely to share phone numbers than younger teens (23% vs. 11%). Focus group participants emphasized that it is too risky to share private password information, which can lead to breaches in security and account hacking.

"My friends do it [share their numbers online], and they'll get texts from a bunch of random people, or a bunch of random phone calls, and I don't really want to deal with it."

-Focus Group Participant, Male, 15-17

The level and types of information that teens disclose online varies depending on the context. Teens with the largest Facebook networks are more likely to share personally identifiable information (i.e., email address and cell phone number) as compared to other teen Facebook users. On commercial websites, teens disclose personal information in exchange for free access, gifts, or other benefits, while 39% of online teens admitted to falsifying their age in order to gain access to websites and online accounts.

Online Privacy/Safety Concerns and Experiences

Many teens report positive experiences online, but some also experience privacy breaches and encounter unwanted content and contact from others. Many youth take actions to protect their privacy (see Appendix C for actions taken by focus group participants to protect their privacy). Focus group participants cited personal experiences, TV shows, and movies (i.e., Catfish and the horror movie Unfriended) as instances that made them wary of over-sharing information. The potential impact on scholarships and job opportunities was an additional concern. Personal experience of privacy breaches can influence teens' online privacy behaviors, and individuals who experience unwanted contact are among the most likely to say that they limit what certain people can see on their profiles.

Four percent of teens reported having posted something online that later caused problems. Older teens ages 14-17 (6% vs. 2%) and older girls (7% vs. 1%) have shared sensitive information that later had consequences for them or a family member. African-American youth (10%) were more likely than white youth (3%) to report that they had posted something that got them in trouble at school (Madden, Lenhart, Cortesi, Gasser, Duggan, Smith, & Beaton, 2013). Teens whose parents use social network sites are also more likely to say that they've gotten in trouble at school because of something posted online. Focus group members highlighted the importance of online reputation management for scholarship and job opportunities.

"There are people that lose their scholarships from inappropriate things that they've posted online."

-Focus Group Participant, Female, 15-17

One in three online teens have witnessed inappropriate online advertising. Exposure to inappropriate advertising online is one of the many risks that parents and other adults are concerned about, but little is known about how often teens encounter ads that they feel are intended for more mature audiences.

Personal experience of privacy breaches influences teens' online privacy behaviors. Twenty percent of teens reported that they have experienced

having a social media or email account compromised. A majority of teens (86%) have taken steps online to remove or mask their digital footprints such as clearing cookies, encrypting email, avoiding using their name, and using virtual networks that mask their Internet protocol address. Many teens reported that they usually figure out on their own how to manage content sharing and privacy settings (Madden, Cortesi, Gasser, Lenhart, & Duggan, 2013).

"My friend gave his password and got hacked. He gave out his password and someone took over his account and I blocked him."

-Focus Group Participant, Male, 13-14

One in six online teens have been contacted online by someone they did not know. Seventeen percent of online teens reported some kind of contact that made them feel scared or uncomfortable. Girls were more than twice as likely as boys (24% vs. 10%) to report unwanted contact. Among social media users, teens who have experienced some kind of unwanted contact online that made them feel scared or uncomfortable were among the most likely to say that they limited what certain friends could see on their profiles (35% vs. 14%).

"I've heard about people that share their location and there are a lot of kidnappers [and strangers] online that could find out where they live and kidnap them."

-Focus Group Participant, Female, 13-14

Online Privacy and Safety Attitudes

Teens care more about threats to social privacy than from corporate and government organizations, and express high levels of confidence in their ability to self-manage. Pew research found that, in the social context of information disclosure, younger teens were more likely to be concerned by potential risks to their physical safety, whereas older teens were more concerned about risks to their reputation. Focus group viewpoints reflect these findings as well:

- **Teens care about social privacy more than the privacy risks posed by third parties** - Contrary to 46% of parents being very concerned about advertiser companies monitoring their child's online behavior, a small minority of teen social media users (9%) say they are "very" concerned about advertisers' access to and use of their personal information.
- **Parental concerns are at odds with teens' confidence in managing their online reputation** - Seventy-two percent of parents of online teens were concerned about how their child manages their reputation online, with half being "very" concerned (49%). Sixty percent of teen Facebook users keep their profiles private, and most report high levels of confidence in their ability to manage their settings. Both boys and girls report similar levels of confidence. Among Facebook users ages 12-13, 41% say it is "not difficult at all" to manage their privacy controls, compared with 61% of users ages 14-17 reporting the same.
- **Younger teens are concerned by risks to physical safety and older teens to reputation** - In terms of information disclosure within the social context, younger teens are more likely to be concerned by potential risks to their physical safety. Older teens expressed awareness that their online activities go beyond the confines of social privacy, which affects their reputation as they pursue educational and employment opportunities. Information sharing and privacy are of particular concern with mobile apps and cell phones—especially among girls—because of location tracking concerns.

Online Privacy and Safety Practices

Few teens embrace a fully public approach in regards to privacy settings, and a lot of effort is dedicated to managing privacy settings and reputation/network management (Marwick et al., 2010). However, when seeking advice—which is often in response to a crisis situation—youth are more likely to turn to peers, friends, and family than go online to search for advice from authority figures (Dresang, 2005). Focus group sessions reported that, if one wished to find advice online, to look in the privacy settings of the app, "Google it", or search on YouTube.

- **Self-management of privacy settings is the primary mechanism to control online access** – Teens primarily control access to their personal information by managing privacy settings. A majority of teen Facebook

users (60%) kept their profiles private. Girls who used Facebook were more likely than boys to have a private profile (70% vs. 50%). The majority of teen Twitter users (64%) were more likely to make tweets public. Teens are increasingly using peer-to-peer anonymous-sharing apps to maintain privacy and minimize the potential risk for harm.

- **Teens' online reputation management requires considerable efforts within network management** – Preferred actions include pruning and revising profiles [deleting or editing posts (59%), deleting comments from someone (53%), and removing their name from tagged photos (45%)]; deleting or deactivating an entire profile or account (31%); friend curation [deleting someone from their network (74%) or blocking (58%)]; cloaking content (58%); and falsification (26%).

"I don't add anyone if they don't have photos (on Instagram) but if their photos are photos of themselves or something, then I'll accept them but if they're inappropriate, then I won't. I'll just deny them."

-Focus Group Participant, Female, 13-14

- **Teens pay particular attention to managing privacy and safety with mobile devices and apps** - Information and privacy are of particular concern with mobile devices and apps because of location tracking features. About half of teen app users (51%) have avoided downloading apps and turned off tracking features (46%) and a quarter (26%) have uninstalled apps due to privacy concerns. Location information is especially sensitive to teen girls and a majority reported disabling location-tracking features on cell phones and apps because they are concerned about access to that information.

"There's usually help in the privacy settings on apps. There's a URL to click or I would watch a YouTube video showing you how to do it."

-Focus Group Participant, Female, 15-17

- **Teens are turning to peers and family members for advice** - Seventy percent of teen users have sought for advice on managing their privacy online. Teen Internet users are more likely to have asked for advice from a friend or peer (42%), parent (41%), or sibling/cousin (37%) rather than consulting a website (13%). Online information behaviors involved using search engines (i.e., Google) and online content platforms (i.e., YouTube). Only 9% have asked a teacher, and 3% have gone to some other person or resource for advice.

Peer-to-Peer Education

The majority of peer education programs and analyses focus on in-person—often in classroom—education methods. While research findings on digital media peer education are limited, many programs are beginning to incorporate social media and web-based information.

Common areas of peer education often involve sensitive topics such as education around sexual health promotion, HIV prevention, substance use, diet/exercise, and reproductive health. As seen in teens' online activities and their thoughts around digital privacy and security, such content can benefit from effective peer education models focusing on sensitive information (Alford, 2011a).

- **Peer-to-peer education positively impacts behavioral change and health outcomes** – Numerous studies and meta-analyses describe the positive change in health outcomes from programs using peer education. These changes include improved health behaviors, seeking appropriate health care, diet and exercise; reduced substance use and abuse (alcohol, cigarettes, marijuana, and other drugs) (Carroll & Kirkpatrick, 2011); reduced sexual risk behaviors (increased contraceptive use, improved communication between partners, increased healthy relationship skills, increased incidence of HIV and STI testing and sharing of results) (Bulduk & Erdogan, 2012); and increased physical safety (peer-to-peer messages increasing seat belt use among minority youth, dating violence) (Ball, Tharp, Noonan, Valle, Hamburger, & Rosenbluth, 2012).

- **Youth respond well to structured health promotion messages and strategies developed by their peers** – Peer-to-peer messaging, often used in youth participatory research, is emerging as an effective way to foster change in youth behavior. Having youth select applicable topics and form their own message creates more accessible and credible information for targeted teen groups. One study found that youth became empowered using new digital and media literacy skills to transform their knowledge into a public message (Beheshti, 2012). Youth-developed messages foster social responsibility, civic engagement, and improved problem-solving skills among peers.

- **The strongest evidence for peer education program effectiveness came from programs that were well designed, properly implemented, and successfully carried out** – In a meta-analysis of 28 peer education in-person programs, these characteristics were common among the programs that achieved the most significant evidence of the positive impact of peer education. Most programs were entirely peer-led, but a few programs merely incorporated peer work as one component of the program.

- **Youth participatory research can make information more accessible and applicable to youth** – Youth participatory research (YPAR), in which youth are included in all stages of research, can help design programs that are geared toward youth. YPAR approaches have been effective in health promotion interventions to varying degrees, including youth sexual violence prevention, digital harassment, and sexual health education (Cook-Craig, 2012; Alford, 2011a).

Knowledge, Attitudes, & Behaviors toward Online Privacy/Safety

This section provides a contextual understanding of teens' knowledge of, behaviors, and attitudes towards online privacy and safety. It draws on the work of danah boyd and a literature review conducted by the Berkman Center for Internet and Society, including other published works.

- **Social media enables teens to extend and reinforce real-world peer relationships** - Youth primarily use social media to reinforce pre-existing relationships. Posting information online is a way for youth to express themselves, connect with peers, increase their popularity, and bond with friends and peers. As a result, social media and mobile technologies play key roles in enforcing both individual friendships and peer group relationships.

- **Teens' privacy norms vary according to the social context of their platform preferences** – The migration of teens away from Facebook stems from the frustration they experience when adults "invade" teen spaces. In an attempt to achieve privacy, teens are moving to newer sites and apps to avoid adults. Young people want to be able to restrict non-peers from viewing information they post online within a social context.

- **The "privacy paradox" states that teens tend to first disclose and then evaluate consequences** - The way teens learn how to manage privacy risk online is often very different from how adults approach privacy management. In what the researchers refer to as the "privacy paradox", teens tend to first disclose and *then* evaluate the consequences, while most adults think first and then ask questions (Barnes, 2006). The process is more experiential in nature for teens, and suggests that there is a disconnect between the privacy concerns of teens and the information they choose to disclose (Jia et al., 2015).

- **Teens' online practices appear risky to outsiders but are normative within a peer context** – Parents' perception that young people put themselves at risk through online activities minimizes the diverse experiences of young people who are online. Youth are often compelled to interact online to ensure full social engagement and participation with their peers. As a result, teens often appear to engage in online

behaviors that violate "privacy", but these actions may actually be normative within a peer context.

- **'Privacy' is a continuum along which teens adopt a 'risk-benefit' approach to sharing** - Choosing what to conceal or reveal is an intense and ongoing process for teens. Within a social context such as a peer group, the anticipated social benefits of online sharing outweigh any potential risks. In contrast, the approach to information disclosure on commercial websites is significantly related to an individual's trust of a particular website or a benefit that they expect to receive in exchange.

- **Teens explore techniques to control meaning of content to achieve privacy in public** – Teens limit what their audience can understand by encoding hidden meaning within their online messages, a practice known as "social steganography". This involves leveraging shared knowledge and cues embedded in particular social contexts with the use of linguistic and cultural tools, including lyrics, inside jokes, and culturally specific references. Another popular practice—subliminal tweeting or "subtweeting"—refers to the practice of encoding tweets to render them meaningless to outsiders.

- **Age and gender are key variables in understanding teens' privacy attitudes and behaviors** - The likelihood of providing personal information online increases with age. Parents are less likely to monitor the Internet use of older teens, and regulated mediation loses its effectiveness with age. Girls are more likely to be concerned about privacy and feel more vulnerable to privacy risks. Boys are more likely to disclose personal information, take risks, and avoid privacy protective behaviors, but also more likely to post fake information on profiles.

- **Teens' concerns, perception of risk, and sense of vulnerability influence privacy practices** - Teens are more likely to engage in privacy-protecting behaviors if they are concerned with privacy, perceive information risk, or see themselves as vulnerable. Typical privacy-protecting behaviors that teens employ include managing privacy settings, obfuscation, refusal to provide information, provision of false information, maintenance of multiple profiles on social media sites, flaming, and circumventing age restrictions.

- **Parental involvement or mediation of online behavior can be viewed as limiting privacy** - Internet monitoring and keylogging (the use of a computer program to record every keystroke of a user) are viewed by youth as snooping and a violation of their privacy, much like searching their school bag, reading their diary, or listening in on a phone call. Parents who attempt to check their children's online journals or social network sites are seen as controlling, invasive, and "clueless". Parents joining Facebook are seen as intrusive and embarrassing.

- **Concepts of privacy in offline settings can affect youths' "online" attitudes and practices** – Traditionally, the home has been seen as "private" space and the "family" as a privately regulated sphere. The "home" is further fragmented into sections; living and family rooms are more 'public', while children's bedrooms are conceptualized as individual and private. The extent to which the computer in a home is public affects the way it is used.

- **Teens' online "boundary marking" tactics are the equivalent of a 'keep out' bedroom door sign** - Strategies the youth use to maintain their privacy from parents while accessing email, chat rooms, and web pages include using multiple email addresses and instant messenger/chat room accounts, writing messages to peers in text-speak, usage of passwords, and window minimization. Teens often develop workarounds and backchannels to connect with each other.

- **Researchers recommend active parental mediation over direct parental intervention** - Parents who use direct intervention (i.e., use of parental controls, setting up privacy settings) may have a suppressive effect on teens. While direct intervention reduces exposure to online risks, it also limits the ability to engage with others online and to learn how to effectively cope with online risks. It may be more beneficial for parents to use a consultative approach through active mediation (i.e., talking with children about what they post) to protect teens from severe online risks, while simultaneously empowering them to engage with others online and learn to make good online privacy choices.

Peer Advice on Management of Online Privacy/Safety

This section discusses the advice that teens (13-17) from the focus groups would give peers and younger individuals on management of online privacy and safety.

Participants spoke about how the Internet can be unsafe and that self-protection is key.

"I would say that the Internet can be unsafe at times and to watch everything you put online, and to also be careful on what information or pictures you post."

-Focus Group Participant, Female, 15-17

Teens also advocated for the avoidance of strangers. Youth should control the amount of personal information disclosed when meeting new people online.

"I would advise not to give too much personal information. When meeting new people online you never know who they really are or what their intentions may be. People can use your personal information to steal your identity or stalk you, as well as many other dangerous things. Practicing limiting yourself to only sharing your name is a good practice for young people using the Internet."

-Focus Group Participant, Male, 15-17

Some teens expressed the need to "self-filter". Teens stated that once something is online—even after deletion—it might remain online forever.

"When you're using the Internet, you need to be extremely careful about what you upload or say. Things you post on the Internet will be there forever, and even if you do delete it someone could have a screenshot of it."

-Focus Group Participant, Female, 13-14

Concerns over exposure to inappropriate online searches were also discussed.

"Be careful what you search on Google; even something that seems innocent could bring up bad stuff."

-Focus Group Participant, Male, 13-14

Focus group participants also spoke about recommendations to keep sensitive information private, even if you consider someone a friend.

"Be cautious of who you talk to and what information you give, especially for the younger kids because they are not mature enough and not experienced with the Internet and social media. Don't give credit card numbers and social security numbers to any website unless it is certified."

-Focus Group Participant, Male, 15-17

Focus group participants defined sensitive information as: date of birth, last name, email address, home address, phone number, current location, and social security number.

“I would say to not give out as much personal info as possible. Age and name is really as far as you should go. Even if someone is your friend, if you don’t know them personally, don’t give out information like that.”

-Focus Group Participant, Male, 13-14

V. DISCUSSION

The networks that emerge as a result of the intersection of people, technology, and practice have significance and implications for teens online. Teens are far removed from the concerns that parents have regarding their children's engagement with social media. Research shows that teens actively manage their privacy and safety in these networks, albeit in ways that differ from privacy standards set by their parents or guardians. The clear distinction that adults fail to make is that informational privacy—of which third-party access is a huge part—is not as big an issue for teens as social privacy. In addition, recognizing a teen's need for privacy and autonomy within the social context is important in understanding their relationship to social media, as well as the privacy strategies that they implement in order to counter the power dynamic that emerges through surveillance.

This is not to say that informational privacy is not a valid concern to teens. Some teens may not see the importance of their data being accessible online, but this is perhaps because they often fail to grasp what happens with that data after it has been posted. Secondly, teens tend to see their data as disconnected individual pieces instead of the metadata that third parties extract value from and seek to monetize. Teens also state that they have "nothing to hide" in order to prove that it would not matter to them if third parties use their data. While youth understand that their data is used for profiling and targeted advertising, they do not necessarily perceive this to be as much an intrusion of their privacy as surveillance by parents.

From a technological perspective, information sharing and privacy are a considerable concern with mobile apps. The U.S. Federal Trade Commission checked apps for state privacy policies and found that 20% (81) of apps provided little or no information about privacy disclosures (FTC Staff Report, 2012). Furthermore, most apps failed to provide any information about the data collected, let alone the type of data collected, the purpose of the collection, and who would obtain access to the data (similar findings were made by Lia, Alford & Coffin, 2012 and Mohapatra & Hasty, 2012). Many of the apps contained interactive features such as advertising (58%, n = 230), the ability to make in-app purchases (17 %, n = 66), and shared certain information such as device ID, geolocation, or phone number (60%, n = 235) without disclosing these practices prior to the downloading of the app.

In a mediated world, researcher danah boyd posits that teens are more likely to question whether information to be shared is intimate enough to require special protection rather than whether it is significant enough to be broadly publicized. In other words, when participating in networks, many participants embrace a widespread public-by-default, private-through-effort mentality (Youn, 2005). Because of this, most teens won't bother to limit the audience who can see what they consider to be insignificant. Teens feel as though their audience can filter out anything that appears to be irrelevant. However, when

youth think that something might be sensitive, they often switch to a different medium such as text messages or chat to communicate with smaller audiences directly.

Research also shows that teens generally rely on themselves to self-manage day-to-day privacy. When they do seek outside help, teens report that they most often turn to friends, siblings, and parents (Forte, Dickard, Magee, & Agosto, 2014). Teens often view their peers as credible because they have had similar experiences, and this can reinforce messages and behaviors. Thus, peer education models on digital privacy and safety can impact attitudes, norms, knowledge, behaviors, and health outcomes. A drawback when relying on peers for advice is the quality of their advice. Peers are not necessarily experts on privacy. Given these concerns, digital privacy and safety education may stand to benefit from peer education programs in multiple settings, and as part of a multi-pronged education strategy.

Although teens report teaching themselves about privacy settings online through search engines like Google or content-sharing platforms such as YouTube, we found that only 13% of teens reported seeking advice online. Even while youth frequently search online for sexual health information (Levine, 2011; Selkie, Benson, & Moreno, 2011), a current search on Google and YouTube does not provide many trusted and current resources on online privacy and safety. Any resources that a Google and YouTube search does yield are not particularly youth-friendly.

Research on how parental privacy concerns and mediation strategies on Facebook influence a teen's privacy concerns and social media privacy practices identified the existence of the *privacy paradox* (Lenhart, 2015). The privacy paradox states that teens tend to first disclose and then evaluate the consequences, while most adults think first and then act. Overall, researchers found that direct parental intervention was associated with teens being more cautious and conservative in their online behaviors. In contrast, parental active mediation gave teens a higher level of autonomy to make more risky disclosure decisions, but also encouraged teens to learn from their mistakes and take corrective actions to protect their online privacy in the future.

An important future research consideration is to recognize that not all young adults are so technologically advanced that young people's digital literacy and information-seeking skills are uniform. Multiple levels of education may be needed to address all skill levels. Other considerations include the method in which parents should speak to their youth about online privacy. Studies have found that, rather than asking the teen questions about their online use, *answering* teens' questions is correlated with higher levels of digital literacy and parental education (Nam & Bishop, 2011). Further research is needed to advance understanding of how social contexts shape and affect information-seeking, as well as how the increased use of emerging digital technologies and information resources are impacting the information-seeking needs and behaviors of teens. For example, teens' online health information-seeking seems to occur out of need or fear rather than proactively, indicating that

although teens may tend to prefer asking people directly, they increasingly access online resources as a result of the Internet's availability, affordability, and anonymity (Dresang, 2005).

VI. RECOMMENDATIONS FOR ONLINE YOUTH PRIVACY COMPETITION AND CAMPAIGN

These research findings have informed the development of key concepts and messages for online privacy and safety. These key concepts will be used to both design and promote a video challenge competition targeted at youth, as well as outreach for a national online campaign. For examples of peer video campaigns and competitions, see Appendix D. Proposed considerations for designing and implementing an online privacy and safety video competition and awareness campaign include:

- Interest categories based on factors that may include teen demographics (i.e., gender, age) and privacy concerns (i.e., social privacy, mobile apps, security threats).

- Thematic categories based on standard control mechanisms (i.e., technical affordances), influencers (i.e., human, online), and innovative strategies (i.e., controlling meaning).

- Promotional outreach through preferred information (i.e., visually-oriented, humorous) and communication modes (i.e., short video format) and channels (i.e., Instagram, Vine, YouTube).

- Message concepts that appeal to the emotions of different teens (i.e., physical safety, digital reputation management, hacking) and that embed language that teens use. Messaging needs to be empowering, not restrictive, creating a trusted environment. Approaches that are defensive and fear-based are often ineffective.

- Campaign resources need to be trustworthy, credible, easily accessible, and offer information in a nonthreatening way. Enhance search engine optimization (SEO) to improve search ranking and the promotion of digital privacy and safety websites.

- Endorsements from celebrities (i.e., Naya Rivera, Drake, Alex from Target, PewDiePie) and respected peer community leaders (i.e., digital literacy) to promote the competition and campaign.

- Popular culture events trigger heightened awareness and interest (i.e., bring risks to life, worst case scenarios) and monitoring for these cultural events will support timely promotional outreach.

VII. APPENDICES

APPENDIX A.

Focus Group Likes/Dislikes of Popular Apps and Social Media Sites

App/Site	Like	Dislike
Facebook	• Games • Family and friend updates • Share location, articles, status and pictures in one place • Privacy settings by audience	• False accounts • Kidnapped • People complain • Primarily for older people/ parents
Twitter	• The new 'Facebook' • Restricted characters=brief tweet • Follow friends, sports, celebrities or funny feeds i.e. Alex from Target and Ian Somerhalder	• Confusing to follow • Required to be public

YouTube	• DIY
	• Resource/ tutorials
	• Shut down strikes
	• Millions of videos
	• Subscribe to favorites such as:
	  • Complex
	  • Fung Brothers
	  • PewDiePie
	  • Yogscast
	  • Captain Sparkle
	  • Vanoss
		• Advertisements
		• Overwhelming to search

Vine	• Funny content • Six-second videos = view more videos • Follow friends or popular videos	• Difficult to search
Oovoo	• Friends + videos • Connect with people that don't have iPhones with FaceTime	• Random requests
Skype	• Chat or audio options • International capabilities • Available on all mobile devices • Connect with family and friends • Video games • Alternate to Teamspeak	• Spam • Hackers • Crash/Error messages
iMessenger	• Built into phone	• Harder to leave group chat

APPENDIX B.
Focus Group Online Information Sharing Practices

	Female, Ages 13-14	Male, Ages 13-14	Female, Ages 15-17	Male, Ages 15-17
	Total (5)	Total (5)	Total (5)	Total (6)
Posted your interests such as movies, music, or books you like	4	5	5	5
Posted information in exchange for free gift or special offer	0	0	1	0
Posted a pic of yourself	5	4	5	6
Posted a pic of a friend, pet, or family member	5	5	5	4
Posted a video of yourself	3	4	4	3
Post a video of a friend, pet, or family member	0	4	4	5
Posted the name of your school	1	2	2	4
Posted the city or town where you live	1	2	1	3
Posted your email address	1	0	0	1
Posted your cell phone number	0	0	0	2
Posted your birth date	4	1	4	3
Accepted a friend request from someone you do not know	4	1	2	3
Posted your full name	2	1	3	2
Posted your relationship status	3	1	2	4
Posted or given access to your current location	0	0	0	3

APPENDIX C.

Actions Taken by Focus Group Participants Youths to Protect Their Privacy

	Female, Ages 13-14	Male, Ages 13-14	Female, Ages 15-17	Male, Ages 15-17
	Total (5)	Total (5)	Total (5)	Total (6)
Deleted or edited something you have posted in the past	5	5	5	5
Deleted comments from others on your profile or account	5	4	2	5
Removed your name from photos that have been tagged to identify you	2	0	3	2
Deleted or deactivated an entire profile account	1	2	2	4
Deleted people from your network of friends' list	4	4	5	4
Blocked people on social media sites	5	4	4	4
Posted an update, comment, photo, or video you have regretted sharing	0	1	2	2
Decided not to post something because you were concerned it would reflect badly on you in the future	0	4	2	4
Shared inside jokes or cloaked your messages in some way	3	4	1	2
Posted false information like a fake name, age, or location to help protect your privacy	2	2	1	2
Downloaded an app to your cell phone or tablet	5	5	5	6
Avoided certain apps due to privacy concerns	0	5	3	6
Uninstalled an app because you learned it was collecting personal information you did not wish to share	1	2	0	2
Turned off the location tracking feature on your cell phone or in an app because you were worried about the privacy of your information	2	3	4	4
Reported a post or content online that was inappropriate	4	3	1	1

APPENDIX D.
Examples of Peer Video Campaigns and Competitions

One Good Thing
The goal of the OneGoodThing.org project is to eliminate the negativity on the Internet by showing all the great things that people are doing online. With connected technology, One Good Thing says we can make the world (and the Internet) a better place. For this year's Safer Internet Day theme, "Let's create a better Internet together," One Good Thing asked: "Tell us how you're using technology to make the world and the Internet better!"

Childnet
UK-based Childnet has a 2015 film competition challenge to create a short film about Internet safety. It is open to school children ages 7-18 within youth organizations across the UK. Films should showcase the positive and inspiring use of the Internet. In 2014, primary theme winners were 60-second films on "How would you make the Internet a better place for you and your friends?" Secondary theme winners were two-minute films on "What does a perfect online world mean to you?"

Teens Talk Back
Teens Talk Back is a video series from Netsmartz that highlights short video interviews with peers sharing their experiences on current online issues like cyberbullying, social networking, and online gaming. NSTeens uses animated videos and characters to engage the hard-to-reach "tween" audience in order to prepare them for protecting themselves online. Real Life Stories focuses on real experiences of teens that have experienced victimization firsthand, and encourage teens to learn from their peers' mistakes. The site also contains presentation materials to encourage tweens and engage teens, and a prize competition to submit a 30- to 60-second video that answers the question; "What's one thing teens need to know about being safer online?"

i-SAFE
i-SAFE is an Internet safety organization that seeks to educate and empower youth. This organization wants to make young people's Internet experiences safe and responsible by teaching them to avoid dangerous, inappropriate, or unlawful online behavior. X-BLOCK provides a forum for students to hang out, learn about cyber safety, and share their online experiences with others. X-BLOCK provides the i-MENTOR training program to promote online safety among peers grades 5 through 12. i-DRiVE TV hosts 30-minute programs made for students, by students, and features student interviews, discussions with experts, technology profiles, and real-life Internet stories. i-SAFE also lists celebrities who help promote awareness of its activities. The organization is currently seeking 30-second PSAs on Internet safety topics.

Teenangels

Teenangels, founded by cyber-lawyer Parry Aftab as a program of WiredSafety.org, are a group of 13 - 18 year old volunteers that have been specially trained in all aspects of online safety. After completion of the required training, the Teenangels run unique programs in schools to spread the word about responsible and safe web surfing to teens, parents, and teachers. They write columns for websites and become expert public speakers and researchers, and work with companies like Disney and Microsoft. They are also trained by law enforcement agencies.

My Privacy and Me

Office of the Privacy Commissioner in Canada ran a national youth video contest from 2008 to 2011 titled My Privacy and Me. The contest was held to capture the attention of young people and encourage them to talk about how to protect their privacy when they are online and in the real world. Over the years, the competition has offered categories that feature a variety of privacy issues, such as mobile devices, social networking, and targeted advertising. Contest winners' videos are available for 2011, 2010, 2009, and 2008. The program has also created a graphic novel, Social Smarts: Privacy, the Internet, and You, to help young Canadians better understand and navigate privacy issues in the online world.

Common Sense Media

Common Sense Media offers research, tips, and tools related to keeping kids safe. Which privacy settings should you use? What are the ins and outs of parental controls? Get tips on everything from the basics, such as smart usernames, to the big stuff, such as appropriate sharing. The website is primarily targeted at parents rather than teens with advice on how to help kids stay safe online. The site also reviews apps that can help kids learn about online privacy (Privacy Camp; Terms and Conditions May Apply). A video has tips on how parents can protect their kids' personal privacy online (never share private information; always use privacy settings; be courteous online), while another video offers three rules to share with kids to ensure their safety online is never compromised (never talk to strangers; don't over share; and never disclose your location). An animated cartoon teaches kids through Disney characters (Phineas and Ferb) how to stay safe online.

Internet Safety 101

Internet Safety 101, a partnership between Enough Is Enough (an Internet safety organization since 1994) and the U.S. Department of Justice, is a resource and teaching series on the dangers children encounter online. Internet Safety 101 strives to educate and empower parents, educators, and other caring adults with the information they need to effectively protect children from Internet dangers. The program offers resources on the Web 2.0 World, which is a mobile, multidirectional, and multi-media tool. Web 2.0 is a communicative platform that changes where and how we interact, share, and seek information. It also represents a paradigm shift in the way the Internet is used by facilitating creativity, information sharing, online communities, and

collaboration among users. Internet Safety 101 also offers background resources on Social Media, Online Gaming, and Mobile Devices.

Social Project
Social Project (formerly Tagworld, which raised close to $50 million in 2009) is a social networking site that launched in late 2005. The site is focused on the teen and adult social networking market. Similar to MySpace, Social Project lets users create and customize profile pages containing multiple types of multimedia (text, photos, video). Below are some of the safety guidelines for teens that Social Project provides: Never reveal personally identifiable information, do not reply to inappropriate emails or messages, be skeptical about people you communicate with or add as a friend, never meet an online stranger in person, and realize that your posts may live forever online.

On Guard Online
FTC offers OnGuardOnline.gov, a website with advice and tips on how to protect children's privacy and safety online. It includes a video that teaches children what they post online could have an impact on people in the real world. On Guard Online asks youth to think about what they post online, and to ask yourself a few questions before posting anything. How would you feel if your family, your teachers, your coaches, or your neighbors found it? Do you want a message or photo you posted to show up years from now, when you apply for college or a job? Being online is part of your life, so stop and think before you click.

Digital Natives
The Digital Natives project focuses on the key legal, social, and political implications of a generation "born digital" – those who grow up immersed in digital technologies, for whom a life fully integrated with digital devices is the norm. By understanding young people's interactions with digital media such as the Internet, cell phones, and video games, Digital Natives addresses the issues these practices raise, shows how to harness the opportunities that digital fluency presents, and shapes regulatory and educational frameworks in a way that advances the public interest. In collaboration with the Youth and Media project and the Berkman Center's digital media producer, they have created a set of videos inspired by each chapter of John Palfrey and Urs Gasser's book Born Digital.

Youth Spark Hub
Microsoft's Youth Spark Hub, a company-wide global initiative to create opportunities for 300 million youth by 2015, offers 30+ programs including an Online Safety program that provides resources to help stay safe online. Some tips include staying sharp on the Internet at home, top tips for online safety at secondary schools, and an Internet Safety IQ test.

VIII. BIBLIOGRAPHY

Alford, S. (2011a). Creating a strong & successful peer sexual health program. Washington, DC: Advocates for Youth. Retrieved from http://www.advocatesforyouth.org/publications/publications-a-z/1855-creating-a-strong-a-successful-peer-sexual-health-program

Alford, S. (2011b). Peer programs: looking at the evidence of effectiveness, a literature review. Washington, DC: Advocates for Youth. Retrieved from http://www.advocatesforyouth.org/publications/publications-a-z/1856-peer-programs-looking-at-the-evidence-of-effectiveness-a-literature-review

Ball, B., Tharp, A. T., Noonan, R. K., Valle, L. A., Hamburger, M. E., & Rosenbluth, B. (2012). Expect respect support groups: preliminary evaluation of a dating violence prevention program for at-risk youth. *Violence Against Women, 18*(7), 746-762.

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

Beheshti, J. (2012). Teens, virtual environments, and information literacy. *Bulletin of the American Society for Information Science and Technology, 38*(3), 54-57.

Biegler, S. & Boyd, D. (2010). Risky Behaviors and Online Safety: A 2010 Literature Review (Draft). Youth and Media Policy Working Group Initiative, Berkman Center for Internet & Society. Retrieved from http://www.zephoria.org/files/2010SafetyLitReview.pdf

boyd, d. (2014). It's Complicated: The Social Lives of Networked Teens. New Haven, CT. Yale University Press.

Buckingham, D. (2008). Introducing Identity. In Buckingham, D. (Ed.) *Youth, Identity, and Digital Media* (1-24). Cambridge, MA: The MIT Press.

Bulduk, S., & Erdogan, S. (2012). The effects of peer education on reduction of the HIV/sexually transmitted infection risk behaviors among Turkish university students. *Journal of the Association of Nurses in AIDs Care, 23*(3), 233-243.

Carroll, J. A. & Kirkpatrick, R. L. (2011). *Impact of social media on adolescent behavioral health.* Oakland, CA: California Adolescent Health Collaborative.

Cook-Craig, P. (2012). Youth sexual violence prevention. VAWnet, a project of the National Resource Center on Domestic Violence. Harrisburg, PA. Retrieved 04/15/2015, from: http://www.vawnet.org

Dresang, E. T. (2005). Access: The information-seeking behavior of youth in the digital environment. *Library Trends, 54*(2), 178-196.

FTC Staff Report. (2012). Mobile Apps for Kids: Current Privacy Disclosures are Disappointing. Federal Trade Commission. Washington, DC. Retrieved from http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf

Forte, A., Dickard, M., Magee, R., & Agosto, D. E. (2014). What Do Teens Ask Their Online Social Networks? Social Search Practices among High School Students. Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing, ACM Press. Retrieved from http://andreaforte.net/ForteCSCW2014SocialSearch.pdf

Forte, A., Agosto, D., Dickard, M., & Magee, R. (2013). Teenagers' Online Question Asking and Answering Behavior. Position Paper. Workshop on Social Media Question Asking. CSCW 2013 San Antonio, TX. Retrieved from http://andreaforte.net/Forte_SMQAworkshop.pdf

Lia, S., Alford J., & Coffin, R. (2012). FPF Mobile Apps Survey. Future of Privacy Forum. Washington, DC. Retrieved from http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf

Jackson, A. C., & Barnes, K. (2013). Peer-to-peer mentoring among urban youth: the intersection of health communication, media literacy and digital health vignettes. *Journal of Digital and Media Literacy. 1*(2).

Jia, H., Wisniewski, P. J., Xu, H., Rosson, M. B., & Carroll, J. M. (2015, February). Risk-taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (pp. 583-599). ACM.

Lenhart, A. (2015). Teens, Social Media and Technology Overview 2015. Pew Research Center. Retrieved from http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/

Levine, D. (2011). Using technology, new media, and mobile for sexual and reproductive health. *Sexuality Research & Social Policy. 8*, 18-26.

Madden, M., Cortesi, S., Gasser, U., Lenhart, A. & Duggan, M. (2013). Where Teens Seek Online Privacy Advice. Pew Research Center. Retrieved from http://www.pewinternet.org/2013/08/15/where-teens-seek-online-privacy-advice/

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Part 4: Putting Privacy Practices in Context: A Portrait of Teens' Experiences Online. Pew Research Center and Berkman Center for Internet & Society. Retrieved from http://www.pewinternet.org/2013/05/21/part-4-putting-privacy-practices-in-context-a-portrait-of-teens-experiences-online/

Madden, M., Lenhart, A., Duggan, M., Cortesi, S. & Gasser, U. (2013). Teens and Technology 2013. Pew Research Center and Berkman Center for Internet & Society. Retrieved from http://www.pewinternet.org/2013/03/13/teens-and-technology-2013/

Marwick, A. E., Murgia-Diaz, D., & Palfrey, J. G. (2010). Youth, Privacy and Reputation (Literature Review)(SSRN Scholarly Paper No. ID 1588163). Rochester, NY: Social Science Research Network.

Mohapatra, M. & Hasty, A. (2012). Mobile Apps for Kids: Disclosures Still Not Making the Grade. Federal Trade Commission. Washington, DC. Retrieved from https://www.ftc.gov/reports/mobile-apps-kids-disclosures-still-not-making-grade

Nam, C., & Bishop, A. P. (2011, February). This is the real me: A community informatics researcher joins the barrio arts, culture, and communication academy in a health information campaign. In *Proceedings of the 2011 iConference* (pp. 371-378). ACM.

Poland, B. D., Tupker, E., & Breland, K. (2002). Involving street youth in peer harm reduction education: The challenges of evaluation. *Canadian Journal of Public Health*, 344-348.

Selkie, E. M., Benson, M., & Moreno, M. (2011). Adolescents' Views Regarding Uses of Social Networking Websites and Text Messaging for Adolescent Sexual Health Education. *American Journal of Health Education*, 42(4), 205-212.

Shiner, M. (1999). Defining peer education. *Journal of Adolescence, 22*. 555-566.

Stakic, S., Zielony, R., Bodiroza, A., Kimzeke, G. (2003). Peer education within a frame of theories and models of behaviour change. *The European Magazine for Sexual and Reproductive Health. 56*, 4–7.

Turner, G., & Shepherd, J. (1999). A method in search of a theory: peer education and health promotion. *Health Education Research, 14*(2), 235-247.

Wisniewski, P., Xu, H., Carroll, J. M. & Rosson, M. B. (2013). Grand Challenges of Researching Adolescent Online Safety: A Family Systems Approach. In

Proceedings of the Nineteenth Americas Conference on Information Systems.

Wisniewski, P., Jia, H., Xu, H., Rosson, M. B. and Carroll, J. M. (2015). "Preventative" vs. "Reactive:" How Parental Mediation Influences Teens' Social Media Privacy Behaviors. In Computer-Supported Cooperative Work and Social Computing.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86-110.