Child Abuse & Neglect 33 (2009) 857–869

Contents lists available at ScienceDirect

Child Abuse & Neglect

Associations between blocking, monitoring, and filtering software on the home computer and youth-reported unwanted exposure to sexual material online

Michele L. Ybarra[a,*], David Finkelhor[b], Kimberly J. Mitchell[b], Janis Wolak[b]

[a] *Internet Solutions for Kids, Inc., 1820 east Garry Ave. #105, Santa Ana, CA, USA*
[b] *Crimes against Children Research Center, University of New Hampshire, Durham, NH, USA*

ARTICLE INFO

Article history:
Received 9 April 2007
Received in revised form 11 August 2008
Accepted 16 September 2008
Available online 1 November 2009

Keywords:
Internet safety

Sexual material
Prevention
Blocking software

ABSTRACT

Objective: To examine the relationship between the use of preventive software on the home computer and unwanted exposure to sexual material online.
Methods: The Youth Internet Safety Survey-2 was a national, RDD telephone survey conducted in March–June 2005. Eight hundred households (one caregiver and one child between the ages of 10 and 17 years) with home Internet access answered questions pertaining to Internet prevention activities in the household and adolescent behaviors and exposures online.
Results: Unwanted exposure to sexual material occurred in 32% of youth in homes with pop-up/spam blockers and 25% of youth in homes with filtering, blocking, or monitoring software on the home computer, compared to 43% of households without preventive software installed on the home computer. Among otherwise similar youth, pop-up/spam blockers installed on the home computer were significantly associated with 59% lower odds of reporting unwanted exposure to sexual material on the home computer; and filtering, blocking, or monitoring software was significantly associated with 65% lower odds. When data were stratified by youth sex, associations between preventive software and unwanted exposure were similar for boys and girls. When stratified by age, preventive software was associated with significantly reduced risk of unwanted exposure for 10–12-year olds and 13–15-year olds, but not for 16–17-year olds.
Conclusion: Although these correlational analyses are far from providing conclusive evidence that preventive software protects children from unwanted exposure to sexual material online, findings suggest that caregivers of boys and girls 15 years of age and younger who want to reduce the likelihood of unwanted exposure to sexual material on the home computer should consider including preventive software—especially filtering, blocking, or monitoring software—in their Internet safety plan.
Practice implications: Practitioners should partner with caregivers in developing an Internet safety plan, including proactive caregiver-youth discussions about expected Internet behavior appropriate for their household.

* Corresponding author.

0145-2134/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.chiabu.2008.09.015

Introduction

As the Internet has become more popular among young people, child and adolescent health professionals, policy makers, and parents have increasingly become concerned about the potential dangers youth face online. Many people agree that communication technologies such as the Internet have made the world a "better place" and most Internet users view the Internet as a very important source of information (USC Annenberg School Center for the Digital Future, 2004). Nonetheless, the vulnerability of youth to exposures to sexual material online has been a concern of professionals working with children and adolescents since the Internet gained prominence in the late 1990. Policy makers have tried to reduce the risk of unwanted sexual exposures online through regulation and the requirement of filtering and blocking software on public computers (Bryan & McCain, 1998; Kirk, 2007; McCain, 2000). These actions are controversial in the absence of data because of the constitutional implications of restricting the public's access to information online (American Library Association, 2006), as well as the public health implications of restricting access to important and behavior-changing health information by overly sensitive blocking software. Internet safety advocates also have encouraged the use of preventive software on the home computer (Internet Education Foundation, 2003). But, important data are lacking that examine the relationship between preventive software and unwanted exposures online.

Exposure to pornography and youth

An example of unwanted exposure to sexual material online is voiced by a 17-year-old male participant in the Youth Internet Safety Survey-2:

> "*I clicked on a link and did not know what it was. It took me to an underage porn site, which is illegal . . . I know you're not allowed to go to those. It was disguised as a different link*" (Wolak, Mitchell, & Finkelhor, 2006).

The 1-year prevalence rate of unwanted exposure to sexual material online has risen significantly from 25% in 2000 to 34% in 2005 among youth between the ages of 10 and 17 years (Wolak et al., 2006). Although there are no data to support or refute the hypothesis, some posit that exposures to pornography during the critical sexual developmental period of adolescence may lead to deviant sexual development such as sexual callousness (Zillmann, 2000). Preliminary data do seem to suggest that intentional exposure to violent x-rated material is cross-sectionally related to sexual aggression online as well as offline among children and youth 10–15 years of age, with less clear associations for x-rated material that is not violent (Ybarra, Mitchell, Hamburger, Diener-West, & Leaf, submitted for publication). Moreover, although the majority of youth are relatively unaffected, 24% of exposed youth in the Youth Internet Safety Survey-2 report being emotionally distressed by incidents of unwanted exposure (Wolak et al., 2006). Even if exposure to sexual material is not related to negative sexual development outcomes, it appears that for some youth, it has the potential for emotional distress.

Advances in preventive software

Enormous advances in computer technology have been made in the past 5 years, including increases in the sizes of hard drives and memory, faster Internet connections, increased capacity to receive, store and transmit images, and increased access through wireless technologies such as mobile phones and gaming devices (Horrigan & Rainie, 2002; Lenhart, Horrigan, & Fallows, 2004; Lenhart, Madden, & Hitlin, 2005; Rainie, 2005; USC Annenberg School Center for the Digital Future, 2004). These advances have been matched by more aggressive marketing of online pornography sites, including ad-ware and spy ware that secretly install software that directs unknowing users to pornography sites. They also can hijack or install unauthorized links to pornography in legitimate web sites (America Online & National Cyber Security Alliance, 2004; Fox, 2005; Sullivan, 2005). With implications for child Internet safety, this kind of stealth software is often bundled with the types of files youth download from gaming and other sites frequented by youth (Fox, 2005; Sullivan, 2005).

To prevent these exposures to sexual material, preventive software also has advanced in sophistication. New features have been developed including the ability to limit the amount of time a child can spend online, block information that can be uploaded or emailed from the computer to protect a child's privacy (and prevent them from sharing personal information), and youth-'friendly' browsers (Internet Education Foundation, 2003; Mitchell, Finkelhor, & Wolak, 2005; Rubenking, 2006). For example, filtering software typically lists different categories (e.g., cults, gambling) that users tailor by turning on or off based upon their preferences. Then, if the program detects content that is not allowed, it blacks out the offending words in an email or blocks the web site. Monitoring software allows a caregiver to record a child's activities by monitoring computer applications (e.g., instant messages) and web sites visited (Rubenking, 2006). This information can be viewed as a report on the computer or collated and emailed to the parent. Previous research suggests that blocking software can be effective in reducing intentional exposure (Consumer Reports, 2004) as well as unintentional exposure (Mitchell, Finkelhor, & Wolak, 2003) to pornographic material online. With increased sophistication of marketing techniques as well as software features, research examining current software is needed.

Other aspects of Internet safety

To illuminate the role that preventive software plays in reducing one's risk for unwanted exposure to sexual material, other factors that may also contribute protection against unwanted exposure online must be taken into account. Findings

conflict about whether parental involvement and Internet safety rules are associated with less risky Internet behaviors (Fleming, Greentree, Cocotti-Muller, Elias, & Morrison, 2006; Steeves, 2005). For example, in a survey of 692 Australian youth, Fleming et al. (2006) report that youth whose parents do not have Internet safety discussions with them were more likely to engage in less safe behaviors online (Fleming et al., 2006). On the other hand, Livingstone and Bober (2005) report that parental rules and regulations are unrelated to youth Internet safety behavior among 1,511 9–19-year olds surveyed in the UK (Livingstone & Bober, 2005). It is likely that at least in part these differences can be explained by differing outcome measures. Taken together however, it seems that caregiver prevention efforts are not always as effective as intended. With the majority of Internet safety messages targeted at caregivers, understanding their relative influence in reducing the likelihood of unwanted exposure to sexual material for a child is of great importance.

Youth age and sex appear to be additionally important factors related to Internet safety efforts. Older youth are more likely to report an unwanted exposure to sexual material (Mitchell et al., 2003) whereas households with younger youth are significantly more likely to report having preventive software on the home computer (Mitchell et al., 2005). Fleming et al. (2006) note that younger youth appear to be especially likely to engage in risky behaviors online if their parents do not talk to them about Internet safety (Fleming et al., 2006). While boys are significantly more likely to report wanted exposure to sexual material (Ybarra & Mitchell, 2005b), no significant sex differences have been noted in regard to unwanted exposure to sexual material (Mitchell et al., 2003). It may be that preventive software has a differential impact for boys and girls, and older and younger youth.

Identified gap in the literature

With increased sophistication of marketing techniques as well as software features, research examining current software is needed. Moreover, understanding whether preventive software is associated with reduced odds of unwanted exposures over and above a general orientation to Internet safety in the household has implications for policy and consumer education efforts. Finally, understanding whether preventive software is more effective for older or younger youth, or boys versus girls will provide clues about the possible need to tailor Internet safety efforts by youth sex and/or age. Using data from the Second Youth Internet Safety Survey (YISS-2), we will examine these two issues. Previous analysis of the YISS-2 data indicate that use of preventive software is associated with significantly lower odds of wanted and unwanted exposure to sexual material generally (Wolak, Mitchel, & Finkelhor 2007). Preventive software was considered among a variety of other youth characteristics in explaining the odds of exposure to sexual material among all young people. The current paper specifically examines the role that preventive software on the home computer has on preventing unwanted exposure to sexual material on that same computer. It provides details about the types of software used and the proportions of youth with unwanted exposure based on software use on the home computer. It also takes into account whether software was installed before or after incidents of unwanted exposure on the home computer. We hypothesize that protective software will be associated with less unwanted exposure to sexual material even after accounting for other influential factors, including a general orientation towards Internet safety in the household, other online behaviors reported by youth, and so forth. We further hypothesize that households with younger youth may be more likely to have preventive software. Nonetheless, we expect the protective effect anticipated for preventive software to be similar for boys and girls, and older and younger youth.

Methods

YISS-2 was a nationally representative telephone survey of young Internet users conducted between March and June of 2005. The research was approved and supervised by the University of New Hampshire Institutional Review Board and conformed to the rules mandated for research projects funded by the US Department of Justice.

Sampling method

Households were randomly identified via random digit dialing. A target sample size of 1,500 households was predetermined based upon a desired maximum expected sampling error of $\pm 2.5\%$ at the .05 significance level. The response rate was 45% using American Association for Public Opinion Research's recommended equation for calculating response rates (The American Association for Public Opinion Research, 2005).

Data collection methods

One youth and one caregiver, self-identified as the one most knowledgeable about the youth's Internet behavior, were surveyed in each participating household. Eligibility criteria for inclusion in YISS-2 required the youth to be between the ages 10 through 17 years, to have used the Internet at least once a month in the previous 6 months, and to be English speaking. Location of Internet access was left intentionally broad to include youth who accessed the Internet outside of the home (e.g., school, library, etc.). Caregivers provided informed consent for their own and their child's participation. Youth also provided informed assent for participation.

Young people were encouraged to identify a time for the interview during which they could talk freely. Privacy was assured, and young people were told that they could skip any question if desired. Interviews were rescheduled if necessary.

On average, the caregiver interview lasted 10 minutes and the youth interview lasted 30 minutes. Youth who participated received $10.

Sample

Because the current analyses were aimed at understanding the impact preventive software on the home computer may have had on unwanted exposure on the home computer, the sample was restricted to households that had home Internet access as indicated by the caregiver ($n = 1,354$). Additionally, questions pertaining to household Internet prevention efforts (e.g., conversations between the caregiver and child about Internet safety) were added to the survey instrument after data collection commenced. Four hundred fifty-five households who had completed the survey before these questions were added to the survey instrument were dropped from the sample.

The survey asked about three types of Internet victimization: harassment, unwanted sexual solicitation, and unwanted exposure to sexual material. Because of time constraints, the survey methodology allowed for the follow-up of up to two of the three incidents, with priority given to harassment and unwanted sexual solicitations. Thus, if all three incidents were reported by a youth, follow-up questions were not asked about the unwanted exposure to sexual material. Of the 355 youth reporting an unwanted exposure to sexual material online in the restricted sample, 63 also reported both unwanted sexual solicitation and harassment experiences and therefore did not provide follow-up detail about the unwanted exposure incident. Because the answers to the follow-up questions indicating whether the incident occurred on the home computer versus somewhere else were missing (leading to misclassification for incidents occurring on the home computer prevented or not based upon preventive software on the home computer), these 63 youth were excluded from the analyses.

Eligibility criteria for the current study sample was thus: households who had Internet access on the home computer, answered all of the survey questions about household prevention efforts, and youth who did not report all three types of Internet victimization assessed in the survey. Eight hundred households met these criteria.

Measures

Unwanted exposure to sexual material

Two types of unwanted exposure to sexual material were asked of youth: (1) whether they had been on a web site that showed pictures of naked people or of people having sex when the young person had not intended to be on such a site; or (2) whether the young person had opened an email or instant message with advertisements or links to x-rated web sites when the young person had not wanted to receive them. Those who responded positively to at least one of the two questions were categorized as having had an unwanted exposure to sexual material in the previous year.

Because our main inquiry focused on the direct link between preventive software and unwanted exposure to sexual material on the *same* computer, it was necessary to restrict the sample to youth exposed to unwanted sexual material on the home computer specifically. Youth who reported unwanted exposure to sexual material on a computer not at the home ($n = 39$) were classified as un-exposed on the home computer. These youth were not excluded from the analyses examining unwanted exposure on the home computer as they reported not being exposed at home and could therefore be classified as 'not being exposed on the home computer'.

Blocking or filtering software

Youth were asked whether there was "software on the home computer they used most that blocked pop-up ads or spam." They also were asked about whether there was "software that filtered, blocked, or monitored how they used the Internet other than software that blocked pop-ups or spam." Based upon these two questions, three groups of youth were identified: (1) no preventive software on the home computer ($n = 197$); (2) pop-up/spam blocking software on the home computer ($n = 256$); and (3) filtering, monitoring, and blocking software on the home computer ($n = 347$). Youth who reported both types of software on the home computer were included in the third category.

Prevention messages

Caregivers were asked whether they had talked with their children about each of four topics: (1) giving out personal information online (yes/no); (2) responding to offensive or nasty messages (yes/no); (3) talking online about very personal things; (yes/no); and (4) how to deal with x-rated pop-up or spam emails (yes/no). Caregivers were additionally asked to rate how much they trusted their children to use the Internet in a responsible manner [5-point Likert scale: 1 (not at all)–5 (extremely)], and how concerned in general they thought adults should be about young people being exposed to sexual material online [5-point Likert scale: 1 (not at all)–5 (extremely)].

Youth were asked about whether their parents had talked to them about: seeing x-rated pictures (yes/no); people who want to talk to youth about sex online (yes/no); and people who might harass, threaten, or embarrass youth online (yes/no).

Youth were asked "Have you heard of places where you can report situations where adults use the Internet to meet kids or teens and involve them in sexual things?" Caregivers were asked whether they "Have heard of places on the Internet

where you can report cases of children being exposed to sexual material or illegal or offensive sexual solicitations?" Those who responded positively were asked to name a specific place; households in which either respondent was able to name a place to report Internet incidents were compared to all other households.

General Internet use and communication

Youth were asked to report the average number of days per week and hours per day they spent online, as well as the importance of the Internet to themselves [5-point Likert scale: 1 (not at all important)–5 (extremely important)] and their relative expertise on the Internet [5-point Likert scale: 1 (beginner)–5 (expert)]. A summation score was created based upon these four variables. Those who had a score 1 standard deviation or higher were compared to all others as an indication of 'high Internet use.'

Additionally, youth reported whether they had ever, in the last year, engaged in each of the following activities: email (yes/no), instant messaging (yes/no), visiting chat rooms (yes/no), playing games (yes/no), working on school assignments (yes/no), playing music (yes/no), keeping an online journal or blog (yes/no), and visiting a dating site (yes/no). Youth also were asked about whom they communicated with online. Indications of talking with people online whom the youth knew in person (yes/no), as well as those the youth knew only online (yes/no) also were included in the analyses.

Internet behaviors

The following online behaviors were queried of the child: posting personal information (e.g., address, age) (yes/no); sending personal information (yes/no); aggression (either making rude or nasty comments (yes/no), or using the Internet to harass or embarrass someone (yes/no)); talking about sex with someone known only online (yes/no); intentionally looking at sexual material online (yes/no); and downloading files (including music files, pod casts, etc.) (yes/no).

Demographic characteristics

Youth reported their race and ethnicity. Caregivers reported the household income, highest household education, the child's sex, and the child's age.

Analyses

Using Stata7 (StataCorp, 2006), missing data were imputed via best-set regression based upon youth age, sex, race, ethnicity, and general Internet use, as well as household income and education. To protect against imputing data for truly nonresponsive participants, valid data was required for at least 85% of the variables assessed. As such, 36 respondents next were dropped. Less than 1% of data were imputed, with household income being the exception (8.9%, $n = 71$). The frequencies of Internet safety behaviors across households were then reported. Frequencies were reported for the entire sample, as well as stratified by youth sex and age. Potential differences in Internet safety behaviors for boys and girls, and older and younger youth were tested using chi-square tests. Next, household and personal characteristics associated with reporting preventive software on the home computer were examined, with significant differences examined using chi-square tests. Finally, the odds of reporting unwanted exposure to sexual material given the report of preventive software on the home computer at the time of the incident were estimated using logistic regression. To examine the association within the context of other influential factors related to Internet safety (e.g., caregiver-youth discussions about Internet safety, general prevention issues, caregiver–child relationships, youth Internet use and behaviors, demographic characteristics), a multi-variate logistic regression model accounting for these underlying characteristics was estimated. Finally, the sample was stratified by youth sex and age to estimate odds of unwanted exposure to sexual material for boys and girls, and older and younger youth separately. Robust standard errors were used in the logistic regression models to account for lack of independence in answers represented by multiple responders in the same household (i.e., caregiver and child).

Results

Characteristics related to Internet safety behavior

As shown in Table 1, 19% of households ($n = 154$) had heard of places where one could report cases of children being exposed to sexual material. Awareness was similar for households with (19%) and without (19%) youth reporting an unwanted exposure to sexual material online (χ^2 (1) = .003, $p > .05$).

Differences by youth age and sex were observed. Older youth, caregivers of boys, and boys themselves were significantly more likely to report having a talk between the caregiver and child about sexual exposures on the Internet. On the other hand, girls and older youth were significantly more likely than boys and younger youth to report their caregiver had talked to them about people who might talk with the youth about sex online. Girls were more likely than boys to report conversations with their caregivers about people online who might bother, threaten, or harass them. Caregivers of boys were significantly

Table 1
Reported Internet safety behavior by youth age and sex ($n = 800$).

Internet safety behavior	All youth ($n = 800$)	Sex ($n = 800$)			Age ($n = 800$)			
		Male ($n = 401$)	Female ($n = 399$)	Statistical comparison	10–12-year olds ($n = 188$)	13–15-year olds ($n = 340$)	16–17-year olds ($n = 272$)	Statistical comparison
Caregivers report having talked with youth about:								
Giving personal information out online	94.0% (752)	94.3% (378)	93.7% (374)	χ^2 (1) = .1	92.6% (174)	95.0% (323)	93.8% (255)	χ^2 (2) = 1.3
Chatting with people met online	91.1% (729)	90.0% (361)	92.2% (368)	χ^2 (1) = 1.2	88.8% (167)	93.8% (319)	89.3% (243)	χ^2 (2) = 5.4
Dealing with offensive/nasty messages	81.8% (654)	80.1% (321)	83.5% (333)	χ^2 (1) = 1.6	77.7% (146)	85.3% (290)	80.2% (218)	χ^2 (2) = 5.4
About x-rated exposures	80.0% (640)	83.8% (336)	76.2% (304)	χ^2 (1) = 7.2**	75.0% (141)	82.4% (280)	80.5% (219)	χ^2 (2) = 4.2
Talking about very personal things	79.3% (634)	77.6% (311)	81.0% (323)	χ^2 (1) = 1.4	73.4% (138)	83.8% (285)	77.6% (211)	χ^2 (2) = 8.7*
Youth report having heard messages from caregiver about:								
People who might threaten, bother, or harass youth online	57.4% (459)	51.6% (207)	63.2% (252)	χ^2 (1) = 10.9***	53.7% (101)	60.9% (207)	55.5% (151)	χ^2 (2) = 3.1
Seeing x-rated pictures on the Internet	54.1% (433)	59.6% (239)	48.6% (194)	χ^2 (1) = 9.7**	45.7% (86)	57.4% (195)	55.9% (152)	χ^2 (2) = 7.1*
People who want to talk about sex with youth	49.8% (398)	45.4% (182)	54.1% (216)	χ^2 (1) = 6.1*	38.8% (73)	57.4% (195)	47.8% (130)	χ^2 (2) = 17.2***
General prevention issues								
Household can name a place to report Internet incidents	19.3% (154)	17.7% (71)	20.8% (83)	χ^2 (2) = 4.3	15.4% (29)	19.1% (65)	22.1% (60)	χ^2 (4) = 7.4
Adults need not be concerned about online sexual exposures for children	4.9% (39)	6.2% (25)	3.5% (14)	χ^2 (1) = 3.2	4.8% (9)	4.7% (16)	5.2% (14)	χ^2 (2) = .1
Caregiver does not trust child online	5.0% (40)	7.0% (28)	3.0% (12)	χ^2 (1) = 6.7*	5.9% (11)	5.6% (19)	3.7% (10)	χ^2 (2) = 1.5

* $p < .05$.
** $p < .01$.
*** $p < .001$.

less likely to report trusting their child online compared to caregivers of girls. Caregivers of 13–15-year olds were most likely to report having talked to their child about people online who may try to get them to talk them about very personal things.

Characteristics related to using preventive software

Seventy-five percent of youth ($n = 603$) reported some form of preventive software on the home computer. Youth who reported preventive software on the home computer were significantly more likely also to report their caregiver had talked with them about Internet safety issues (Table 2). They also reported higher frequencies of most online activities (e.g., using instant messaging) and many behaviors (posting personal information online, communicating with people known only online). Compared to youth who reported only pop-up or spam blockers, youth reporting filtering, blocking or monitoring software were significantly more likely to report, and to have their caregivers report, having discussions with their children about Internet safety. They were significantly less likely to report high Internet use in general, and using the Internet for communication activities such as instant messaging and blogging. Aggressive behaviors towards others and purposefully seeking sexual material were reported significantly more often by youth with pop-up or spam blockers versus those with filtering, blocking or monitoring software on the home computer. Aside from youth age, households with and without preventive software were generally similar in terms of demographic characteristics. Findings were similar when the 63 youth who were not asked follow-up information about the incident (see *Methods* above) were included in the sample.

Unwanted exposure to sexual material based upon blocking and monitoring software

Of the 253 youth who reported an unwanted exposure to sexual material on the home computer, 20% ($n = 51$) reported not having preventive software on the home computer at the time of the incident and adding software as a result; 18% ($n = 46$) reported having some type of preventive software on the home computer and adding more preventive software as a result of the unwanted exposure; 33% ($n = 83$) had some type of preventive software when the unwanted exposure occurred and did not add additional software; and 20% ($n = 51$) did not have some type of preventive software on the home computer at the time of the incident and did not add preventive software subsequently. Eight percent ($n = 22$) of youth reporting an unwanted exposure were missing data about preventive software and were conservatively coded as not having software on the home computer. A comparison of types of preventive software installed on the home computer suggested that 25% ($n = 88$) of youth reporting monitoring, blocking, or filtering software on the home computer also reported an unwanted exposure to sexual material on the home computer; 32% ($n = 81$) of youth reporting pop-up or spam blocking software on the home computer reported an unwanted exposure. In comparison, 43% ($n = 84$) of youth reporting no preventive software on the home computer also reported an unwanted exposure to sexual material online [χ^2 (2) = 17.4, $p < .001$].

Table 3 displays 12 logistic regression models: unadjusted and adjusted models for all youth, boys, girls, 10–12-year olds, 13–15-year olds, and 16–17-year olds. Adjusted findings take into account demographic characteristics (youth age, sex, race, ethnicity, household education, household income), Internet use (generally high use; using the Internet for emailing, instant messaging, chat rooms, playing games, school assignments, listening to music, blogging, going to dating web sites), online behaviors (talking to friends online, talking to people known only online, posting personal information, sending personal information, aggressive behavior towards others online, talking about sex with someone known only online, purposefully looking at x-rated material, downloading files), and Internet safety characteristics (caregiver-reported Internet safety discussions with child; youth-reported Internet safety discussions with caregiver; household being able to identify where to report Internet crimes, a lack of concern about youth online generally, a lack of trust of the youth online specifically). For all models, "No software" is the reference group.

Findings suggested that both pop-up/spam blockers and filtering, blocking, or monitoring software installed on the home computer were associated with significantly reduced odds of reporting an unwanted exposure to sexual material on the home computer in the pervious year. Associations were not explained by underlying differences in household prevention behaviors, youth demographic characteristics, Internet use, or Internet behavior (see AORs, Table 3). Indeed, the only additional Internet safety behavior significantly related to the report of unwanted exposure to sexual material when examining associations among the whole sample ($n = 800$) was youth-reported discussions with their caregiver about how to avoid people on the Internet that might want to talk to them about sex (AOR = 2.1, $p < .01$).

Results were similar for boys (pop-up/spam blockers: AOR: .32, $p < .01$; filtering, blocking, or monitoring software: AOR: .28, $p < .001$) and girls (pop-up/spam blockers: AOR: .46, $p < .05$; filtering, blocking, or monitoring software: AOR: .42, $p < .01$). When stratified by age however, differences were noted such that preventive software was most strongly associated with reduced risk for 10–12-year olds (pop-up/spam blockers: AOR: .26, $p > .05$; filtering, blocking, or monitoring software: AOR: .14, $p < .001$) and 13–15-year olds (pop-up/spam blockers: AOR: .22, $p < .001$; filtering, blocking, or monitoring software: AOR: .21, $p < .001$), but not for 16–17-year olds (pop-up/spam blockers: AOR: .91, $p > .05$; filtering, blocking, or monitoring software: AOR: .67, $p > .05$).

Youth who reported that the filtering, blocking, or monitoring software was installed on the home computer *after* the unwanted exposure to sexual material ($n = 51$) were coded as not having software at the time of the wanted exposure for the above analyses. It is possible however that the youth were mistaken about the timing of the software installation or for reasons of social desirability bias, indicated that they added the software after the incident when this was not truly the case. As such, subsequent analyses were conducted to examine the impact on the results if these youth were coded differently.

Table 2
Characteristics associated with preventive software on the home computer ($n = 800$).

Personal characteristics	Report of preventive software on the home computer			Statistical comparison			
	No preventive software (25%, $n = 197$)	Software that blocks pop-ups or spam (32%, $n = 256$)	Software that filters, blocks, or monitors how you use the Internet (44%, $n = 347$)	Comparison cross all three categories		Comparison between the two types of preventive software	
	% (n)	% (n)	% (n)	Chi-square test	p-value	Chi-square test	p-value
Caregivers report having talked with youth about Internet safety issues:							
Giving personal information out online	92.9% (183)	93.4% (239)	95.1% (330)	χ^2 (2) = 1.4	.51	χ^2 (1) = .8	.36
Chatting with people met online	89.3% (176)	89.8% (230)	93.1% (323)	χ^2 (2) = 2.9	.23	χ^2 (1) = 2.0	.15
Dealing with offensive/nasty messages	81.7% (161)	78.9% (202)	83.9% (291)	χ^2 (2) = 2.4	.30	χ^2 (1) = 2.4	.12
About x-rated exposures	80.7% (159)	75.4% (193)	83.0% (288)	χ^2 (2) = 5.4	.07	χ^2 (1) = 5.3	.02
Talking about very personal things	79.2% (156)	75.4% (193)	82.1% (285)	χ^2 (2) = 4.1	.13	χ^2 (1) = 4.1	.04
Youth report having heard Internet safety messages from caregiver about:							
People who might threaten, bother, or harass youth online	49.8% (98)	55.5% (142)	63.1% (219)	χ^2 (2) = 9.7	.01	χ^2 (1) = 8.8	.003
Seeing x-rated pictures on the Internet	50.8% (100)	50.0% (128)	59.1% (205)	χ^2 (2) = 6.1	.05	χ^2 (1) = 4.9	.03
People who want to talk about sex with youth	44.2% (87)	44.5% (114)	56.8% (197)	χ^2 (2) = 12.1	.002	χ^2 (1) = 3.6	.06
General prevention issues							
Household can name a place to report Internet incidents	18.8% (37)	19.9% (51)	19.0% (66)	χ^2 (2) = .1	.95	χ^2 (1) = .1	.78
Adults need not be concerned about online sexual exposures for children	3.6% (7)	6.6% (17)	4.3% (15)	χ^2 (2) = 2.7	.26	χ^2 (1) = 1.6	.21
Caregiver–child relationship							
Low caregiver trust of child online	4.6% (9)	5.5% (14)	4.9% (17)	χ^2 (2) = .2	.90	χ^2 (1) = .1	.75
Youth Internet use							
High Internet use	18.3% (36)	34.8% (89)	23.9% (83)	χ^2 (2) = 17.1	<.001	χ^2 (1) = 8.5	.004
Internet activities							
Doing school work	88.8% (175)	93.0% (238)	93.4% (324)	χ^2 (2) = 3.9	.14	χ^2 (1) = .0	.85
Emailing	72.1% (142)	86.7% (222)	82.1% (285)	χ^2 (2) = 16.0	<.001	χ^2 (1) = 2.3	.13
Playing games	85.8% (169)	77.0% (197)	83.6% (290)	χ^2 (2) = 6.9	.03	χ^2 (1) = 4.2	.04
Instant messaging	62.4% (123)	80.5% (206)	70.0% (243)	χ^2 (2) = 18.4	<.001	χ^2 (1) = 8.4	.004
Listening to music	32.0% (63)	46.1% (118)	35.5% (123)	χ^2 (2) = 11.1	.004	χ^2 (1) = 7.0	.01
Chat room use	23.9% (47)	27.3% (70)	27.4% (95)	χ^2 (2) = .9	.63	χ^2 (1) = .0	.99
Blogging	8.1% (16)	23.4% (60)	15.9% (55)	χ^2 (2) = 19.2	<.001	χ^2 (1) = 5.5	.02
Going to dating sites	.5% (1)	.0% (0)	.9% (3)	χ^2 (2) = 2.2	.33	χ^2 (1) = 2.2	.14

Internet behaviors							
Communicate with friends known offline	74.6% (147)	89.1% (228)	82.1% (285)	χ^2 (2) = 16.1	<.001	χ^2 (1) = 5.6	.02
Post personal information	47.7% (94)	60.2% (154)	58.8% (204)	χ^2 (2) = 7.6	.02	χ^2 (1) = .1	.74
Talk about sex with people known only online	3.1% (6)	2.3% (6)	4.0% (14)	χ^2 (2) = 1.4	.50	χ^2 (1) = 1.3	.25
Communicate with people known only online	24.4% (48)	36.3% (93)	30.0% (104)	χ^2 (2) = 8.3	.02	χ^2 (1) = 2.7	.10
Aggressive behavior towards others	24.9% (49)	34.8% (89)	23.1% (80)	χ^2 (2) = 10.9	.004	χ^2 (1) = 10.0	.002
Send personal information	18.8% (37)	27.0% (69)	22.8% (79)	χ^2 (2) = 4.2	.12	χ^2 (1) = 1.4	.24
Download files	11.2% (22)	18.8% (48)	12.1% (42)	χ^2 (2) = 7.1	.03	χ^2 (1) = 5.1	.02
Purposively look for sexual images online	10.7% (21)	16.0% (41)	10.7% (37)	χ^2 (2) = 4.6	.10	χ^2 (1) = 3.7	.05
Demographic characteristics							
Youth							
Age (*M*:*SD*)	14.0 (2.2)	14.15 (2.1)	14.2 (2.0)	F (2) = 4.16	.02	t (601) = 2.0	.05
White race	81.7% (161)	77.0% (197)	79.3% (275)	χ^2 (2) = 1.5	.46	χ^2 (1) = .5	.50
Female	51.8% (102)	53.1% (136)	46.4% (161)	χ^2 (2) = 3.0	.22	χ^2 (1) = 2.7	.10
Hispanic ethnicity	8.6% (17)	9.4% (24)	5.8% (20)	χ^2 (2) = 3.1	.21	χ^2 (1) = 2.8	.09
Household							
Income (<$50,000)	33.0% (65)	30.1% (77)	34.0% (118)	χ^2 (2) = 1.1	.59	χ^2 (1) = 1.0	.31
High school education or less	19.8% (39)	18.0% (46)	17.6% (61)	χ^2 (2) = .4	.81	χ^2 (1) = .0	.90

Table 3
Odds of unwanted exposure to sexual material on the home computer for youth reporting preventive software on the home computer versus youth reporting no preventive software on the home computer.

	Unadjusted models						Adjusted models					
	Pop-up/spam blockers			Filtering, blocking, or monitoring software			Pop-up/spam blockers			Filtering, blocking, or monitoring software		
	OR	95% CI	*p*-value	OR	95% CI	*p*-value	AOR	95% CI	*p*-value	AOR	95% CI	*p*-value
All youth (*n* = 800)	.62	.42, .92	.02	.46	.32, .66	<.001	.41	.27, .65	<.001	.35	.23, .53	<.001
Sex												
Girls (*n* = 399)	.70	.41, 1.21	.20	.52	.30, .90	.02	.46[a]	.23, .90	.02	.42[a]	.23, .80	.01
Boys (*n* = 401)	.55	.32, .96	.04	.39	.23, .66	<.001	.32	.16, .63	.001	.27[b]	.15, .50	<.001
Age												
10–12 yo (*n* = 188)	.45	.17, 1.24	.12	.35	.14, .88	.03	.26[b]	.05, 1.24	.09	.14	.05, .44	.001
13–15 yo (*n* = 340)	.35	.19, .64	.001	.29	.17, .51	<.001	.22[a]	.10, .46	<.001	.21[a]	.11, .42	<.001
16–17 yo (*n* = 272)	1.04	.54, 1.98	.91	.79	.41, 1.51	.47	.91[a]	.41, 2.02	.82	.67[a]	.32, 1.40	.29

[a] Estimates not adjusted for the report of going to dating web sites because of high-collinearity.

[b] Estimates not adjusted for the report of going to dating web sites, playing games online, talking about sex with someone known only online, purposefully looking at x-rated material, or parental report of concern about youth online generally because of high-collinearity.

Findings changed and were no longer significant if these youth were coded as having software at the time of the incident (pop-up/spam blockers: AOR: 1.6, $p > .05$; filtering, blocking, or monitoring software: AOR: 1.2, $p > .05$), or were dropped from the analyses entirely (pop-up/spam blockers: AOR: 1.1, $p > .05$; filtering, blocking, or monitoring software: AOR: .96, $p > .05$).

Discussion

Youth in three of four households reported some form of preventive software installed on the home computer at the time of the survey. Specifically, two in five (43%) of youth-reported blocking, monitoring, or filtering software, and an additional one-third (32%) of youth report pop-up or spam blockers on the home computer at the time of the survey. As reported previously (Wolak et al., 2007), preventive software on the home computer is associated with significantly lower odds of unwanted exposure to sexual material on that computer among YISS-2 survey respondents. Even after adjusting for potentially influential characteristics, the current analyses suggest that the anti-spam and pop-up software was associated with 59% lower odds of unwanted exposure to sexual material and the filtering, blocking, or monitoring software was associated with 65% lower odds of unwanted exposure to sexual material. These results suggest that preventive software on the home computer may have a protective influence against unwanted exposure to sexual material online that occur on the home computer. But preventive software seems insufficient by itself to prevent all unwanted exposures online given that 32% of youth with pop-up and spam blockers, and 25% with filtering, monitoring, and blocking software installed on the home computer still reported an unwanted exposure to sexual material. We also add a cautionary note for the reader: given the rapidly changing nature of the technology environment, it is hard to generalize results too far past the date of the survey.

Contrary to expectations (Livingstone & Bober, 2005; Mitchell et al., 2005), the report of preventive software on the home computer increased with youth age in the current sample. It may be that while parents are reducing the number of restrictions placed on Internet use as the child gets older (Livingstone & Bober, 2005), they are off-setting this with the installation of preventive software. Stratified analyses suggested however, that neither pop-up/spam blockers nor filtering, monitoring, or blocking software was associated with reduced odds of unwanted exposure to sexual material for older teens (i.e., 16–17-year olds). Filtering, blocking, and monitoring software was associated with 86% lower odds of unwanted exposure to sexual material among otherwise similar children aged 10–12 years old and 88% lower odds among otherwise similar children aged 13–15 years old. Although these are correlational findings, the data are consistent with a protective effect from the software and suggest that caregivers of boys and girls 15 years of age and younger who want to reduce the likelihood of unwanted exposure to sexual material on the home computer should consider including preventive software in their Internet safety plan, especially filtering, blocking, or monitoring software. Other factors seem likely more influential in explaining the odds of unwanted exposures among youth 16 years of age and older.

Household characteristics of preventive software users

Consistent with previous research (Mitchell et al., 2005), households with youth reporting preventive software also were more likely to report other behaviors related to a general orientation towards Internet safety, and this appeared to be especially true for youth reporting filtering, blocking, or monitoring software. This suggests that the use of preventive software is sometimes done in concert with other prevention techniques by the caregiver. Thus, those who use preventive software may be more safety conscious in general. It is possible that households where caregivers and youths are more computer-savvy, know how to install the software, or are more aware of the risks related to Internet use also are less likely to experience unwanted exposures simply because of their increased savvy. Nonetheless, even in the context of these underlying differences in household Internet safety tactics, preventive software appeared to play a preventive role in reducing the odds of unwanted exposure to sexual material on the home computer.

It should be noted that although half of all youth and 80% of all caregivers reported conversations with each other about Internet safety topics, these discussions were not associated with a significant reduction in odds of also reporting unwanted exposure to sexual material once other influential factors are taken into account. Indeed, youth-reported discussions with their caregiver about how to avoid people on the Internet who might want to talk to them about sex were associated with twofold increased odds of also reporting unwanted sexual material. Moreover, one in five (20%, $n = 51$) youth exposed to unwanted sexual material reported installing preventive software after it happened. These two findings suggest that it is not uncommon for parents to have discussions with youth and install software in reaction to risk situations. Caregivers should be encouraged instead to be proactive and use preventive software and have discussions with their children about navigating the Internet safely before unwanted incidents occur.

One in five households (19%) had heard of places where one could report cases of children being exposed to sexual material online. While encouraging, this suggests that four out of five households do not know where to report online incidents. Given that households with youth reporting unwanted exposures to sexual material were no more likely to know where to report these types of incidents, we must do a better job of providing specific information about where to report such incidents for youth and their caregivers (e.g., CyberTipLine.com).

A note about "unwanted"

Although exposures were described by the child as 'unwanted,' not all of them were inadvertent or involuntary (Wolak et al., 2006). Seventeen percent of youth who reported an unwanted exposure in the current analyses indicated they could tell it was an x-rated web site before they clicked on the link in the email or entered the web site. For some youth, it appears that exposures to sexual material can be somewhat volitional yet still unwanted when they occur. It is possible that although the youth was expecting to see x-rated material, the actual content was not expected and therefore unwanted. For example, perhaps they were expecting to see "soft porn" and were instead shown "hard porn" or other unexpected pictures (e.g., bestiality). It also is possible that while the youth "knew" that it was x-rated, the youth did not have a concrete sense of what "x-rated" meant. Often, we use words and phrases around young people and assume that they know what these phrases mean without defining them. This is supported by a recent finding that 41% of youth between the ages of 10 and 15 years report not knowing what an "x-rated web site" is (Ybarra et al., submitted for publication).

Determining temporality

Six percent of all youth in the analytic sample ($n = 51$, 7% of youth reporting preventive software at the time of the survey) reported installing filtering, monitoring, or blocking software on the home computer *after* an unwanted exposure to sexual material on the home computer occurred. These youth were influential in our findings. If they were coded as "having software" on the home computer, or dropped from the analyses entirely, neither type of preventive software was significantly protective. It is possible that if too many youth with unwanted exposure were recoded as not having software than was truly the case (for example, wanting for social desirability reasons to suggest that action was being taken to prevent recurrence, they said that it was installed afterward), this would result in the detection of an artificial association. One clear way to deal with this is through an experimental design that would assign software to households on a randomized basis. Researchers could recruit households who are willing to have research software installed on their computer that would communicate to the researchers any changes to the software programs on the computer as well as where the users go online. Another option would be to design a longitudinal study whereby at short time periods (e.g., every other month, every 6 months) over several years, youth were asked whether preventive software had been added to the computer and whether they had experienced unwanted exposure to sexual material. This would be potentially a very costly study.

Policy implications

The current findings provide support for the suggestion that preventive software be used on the home computer to help prevent unwanted exposures to sexual material online. As this is a correlational study however, findings need to be tested in an experimental design to conclusively determine whether the installation of software on the home computer reduces unwanted sexual experiences online. These data provide a foundation from which to investigate the effects of preventive software on public computers in reducing the risk of unwanted exposure to sexual material. Given the constitutional implications of restricting the public's access to information online (American Library Association, 2006), as well as the public health implications of restricting access to important and behavior-changing health information by overly sensitive blocking software, caution continues to be warranted.

Limitations

Of greatest importance, the rapidly changing nature of the technology environment makes it hard to generalize results too far past the date of the survey. This is especially true given advances and availability of Internet-capable phones, Internet-connected gaming consoles, and so forth. since the data were collected in 2005. Moreover, data collection occurred around a time of noted increase in spyware and illegal music piracy that had spyware hidden within (e.g., Kazaa) (Anti-Spyware Coalition, 2006). Most of these sites have been shut down by the courts since that time. It is possible that a lower prevalence of exposure via pop-ups and spyware would be observed by a similar survey today. Furthermore, the use of blocking, monitoring, and filtering software on the home computer was queried in the same question. These three types of software were placed together because of focus group findings suggesting youth perceived these to be much the same thing. It is possible that if each type of software were queried separately, differences between them in their ability to prevent unwanted exposure to sexual material may be seen. It also should be kept in mind that only the most distressing or recent exposure was queried further. It is possible that preventive software was installed as a result of another incident and failed to prevent the exposure discussed. If true, this would likely attenuate the findings. Also, we did not assess the level of certainty respondents had about the existence of software on the home computer; it is possible that not all respondents are aware of all of the software on their computer, especially software that was preloaded. Additionally, it is possible that youth who report a lack of exposure to sexual material also are more likely report the presence of preventive software. All types of self-reported data are vulnerable to self-report bias. Nonetheless, youth self-reported data are commonly relied about to draw inferences about health and risky behaviors, and to inform public health and policy (US Department of Health and Human Services, 1999; US Department of Health and Human Services, 2002). Finally, the current analyses focus exclusively on unwanted

exposures to sexual material. Readers interested in examinations of youth reporting wanted exposures to sexual material are referred elsewhere (Wolak et al., 2007; Ybarra & Mitchell, 2005a).

Conclusions

The Association for Library Service to Children and the Public Library Association (Helms, 2003) notes that, although blocking software may prevent viewing some objectionable content, nothing is a replacement for parent–child interaction in the online world. It is certainly true that blocking software is not a panacea. Thirty-two percent of youth with pop-up and spam blockers, and 25% with filtering, monitoring, and blocking software on the home computer report an unwanted exposure to sexual material. Preventive software appears necessary but is an insufficient tool if used alone in the greater arsenal of a household Internet safety plan. Future research should examine the role that other new technologies, such as cell phones, may have on increasing unwanted exposures to sexual material for youth.

References

America Online & National Cyber Security Alliance. (2004). AOL/NCSA Online Safety Study. http://www.staysafeonline.info/pdf/safety_study_v04.pdf.
American Library Association. (2006). CIPA Legal History. http://www.ala.org/ala/washoff/WOissues/civilliberties/cipaweb/legalhistory/remarks.htm.
Anti-Spyware Coalition. (2006). http://www.antispywarecoalition.org/.
Bryan, R., & McCain, J. (1998, October). Children's Online Privacy Protection Act (COPPA). 105 S. 2326, 6501–6506.
Consumer Reports. (2004). Consumer Reports investigates how to protect against spam, spyware, and phishing. http://www.consumerreports.org/cro/cu-press-room/pressroom/eng0409spm.htm?resultPageIndex=1&resultIndex=1&searchTerm=blocking%20software.
Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A., & Morrison, S. (2006). Safety in cyberspace: Adolescents' safety and exposure online. *Youth & Society*, *38*, 135–154.
Fox, S. (2005). *Spyware: The threat of unwanted software programs is changing the way people use the Internet*. Washington DC: Pew Internet & American Life Project.
Helms, C. H. (2003). Children and the Internet: Policies that work. http://www.ala.org/ala/alsc/alscpubs/childrentheinternetpoliciesthatwork/ChildrenInternetArtTwo.htm.
Horrigan, J., & Rainie, L. (2002). *The broadband difference. How online Americans' behavior changes with high-speed Internet connections at home*. Pew Internet Life Project.
Internet Education Foundation. (2003). GetNetWise. GetNetWise.com.
Kirk, M. (2007, February). Deleting Online Predators Act of 2006 (DOPA). H.R. 1120.
Lenhart, A., Horrigan, J., & Fallows, D. (2004). *Content creation online. 44% of U.S. Internet users have contributed their thoughts and their files to the online world*. Washington DC: Pew American Life Project.
Lenhart, A., Madden, M., & Hitlin, P. (2005). *Teens and technology: Youth are leading the transition to a fully wired and mobile nation*. Washington DC: Pew Internet and American Life.
Livingstone, S., & Bober, M. (2005). *UK kids go online: Final report of key project findings*. London: London School of Economics and Political Science.
McCain, J. (2000, December). Children's Internet Protection Act (CIPA) (pp. 106–554).
Mitchell, K., Finkelhor, D., & Wolak, J. (2003). The exposure of youth to unwanted sexual material on the Internet: A national survey of risk, impact, and prevention. *Youth & Society*, *34*, 330–358.
Mitchell, K., Finkelhor, D., & Wolak, J. (2005). Protecting youth online: Family use of filtering and blocking software. *Child Abuse & Neglect*, *29*, 753–765.
Rainie, L. (2005). *16% of Internet users have viewed a remote person or place using a web cam*. Washington DC: Pew Internet & American Life Project.
Rubenking, N. J. (2006). Buying guide: Parental controls. http://www.pcmag.com/article2/0,1759,1954772,00.asp.
StataCorp. (2006). *Stata statistical software (version release 9.0) [computer software]*. College Station, TX: Stata Corporation.
Steeves, V. (2005). *Young Canadians in a wired world: Phase II*. Ottawa: Media Awareness Network.
Sullivan, B. (2005). Spyware firms targeting children. Pop-ups pile up after visiting kids' sites. *MSNBC*.
The American Association for Public Opinion Research. (2005). Standard definitions: Final dispositions of case codes and outcome rates for surveys. http://www.aapor.org/pdfs/standarddefs_3.1.pdf.
US Department of Health and Human Services. (1999). *Mental health: A report of the surgeon general*. Rockville, MD: US Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Center for Mental Health Services, National Institutes of Health, National Institute of Mental Health.
US Department of Health and Human Services. (2002). Risk factors for youth violence. In *Youth violence: A report of the surgeon general*. Washington, DC.
USC Annenberg School Center for the Digital Future. (2004). *Ten years, ten trends* (Rep. No. Year 4).
Wolak, J., Mitchell, K., & Finkelhor, D. (2006). *Online victimization of youth: 5 years later* (Rep. No. 07-06-025). Alexandria, VA: National Center for Missing & Exploited Children.
Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Unwanted and wanted exposure to online pornography in a national sample of youth Internet users. *Pediatrics*, *119*, 247–257.
Ybarra, M., & Mitchell, K. (2005a). Adolescent pornography exposure on the Internet: A national survey. *Cyberpsychology & Behavior*, *8*, 473–486.
Ybarra, M., & Mitchell, K. (2005b). Exposure to Internet pornography among children and adolescents: A national survey. *Cyberpsychology & Behavior*, *8*, 473–486.
Ybarra, M., Mitchell, K., Hamburger, M., Diener-West, M., & Leaf, P. (submitted for publication). X-rated material and sexually aggressive behavior among adolescents: Is there a link? *Aggressive Behavior*.
Zillmann, D. (2000). Influence of unrestrained access to erotica on adolescents' and young adults' dispositions towards sexuality. *Journal of Adolescent Health*, *27*, 41–44.