Youth Internet Safety Task Force

Compilation of Current Research

Sept 1, 2010

Table of Contents

McAfee Survey Results: The Secret Lives of Teens Online..3

The Future of Internet Safety Education: Critical Lessons from Four Decades of Youth Drug Abuse Prevention..4

Risky Behaviors and Online Safety: A 2010 Literature Review (DRAFT).................................4

Berkman Center Sexting: Youth Practices and Legal Implications 5

PEW Teens and Mobile Phones 6

PEW Cyberbullying 2010: What the Research Tells Us 7

PEW Social Media and Young Adults 7

NCSA Study: Too few schools are teaching cyber safety..7

Microsoft Online Reputation in a Connected World 8

How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?...9

PEW Reputation Management and Social Media..10

Yahoo: Child Safety Study 11

Norton Online Family Report Global insights into family life online 12

Youth Safety on a Living Internet: 13

Cyberbullying Research Summary: Cyberbullying and Suicide 15

The School Bully in Cyberspace 16

Home Broadband 2010..16

Generation M^2 Media in the Lives of 8 to 18 year-olds 17

McAfee Threats Report: Second Quarter 2010 18

Privacy Online: Fair Information Practices in the Electronic Marketplace 18

Prepared Statement of the Federal Trade Commission on Consumer Privacy.......................19

McAfee Survey Results: The Secret Lives of Teens Online

June 22 2010

Excerpt

"The Secret Life of Teens," is a new survey conducted online by Harris Interactive research for McAfee and provides insight into how youth ages 10-17 are using the net today.

Key findings:

Sharing personal information

- 69% of 13-17 year olds have updated their status on social networking sites to include their physical location
- 28% of teens chat with people they don't know in the offline world -- 43 percent shared their first name
- 24% percent shared their email address
- 18% percent shared a personal photo of themselves
- 12 %percent shared their cell phone number
- Girls are more likely than boys to chat with people online that they don't know in the offline world, (32% vs. 24%)
- 13-15 year old girls (16 %) are more likely than boys the same age (7%) to have given a description of what they look like.

Cyberbullying

- Nearly 50% of Teens Don't Know What to Do if Cyberbullied
- One-in-three teens knows someone who has had mean or hurtful information posted about them online
- 14% of 13-17 year olds admit to having engaged in some form of cyberbullying behavior in 2010

Access:

- 87% of teens go online somewhere other than at home
- 54% access from their friends' or relatives' houses
- 30% of teens access the Web through a phone and 21% through a video game system
- 23% of kids go online anywhere with an open Wi-Fi signal

Teens Hide What They're Doing Online

- 42% don't tell their parents what they do while they are online
- 38% of teens close or minimize the browser when their parents enter the room
- 32% of teens clear the browser history when they are done using the computer
- 55% of 13-17 year olds hide what they do online from parents

Kids to Blame for Infected Family PC?

- More than a quarter of teens (27%) accidentally allowed a virus, spyware, or other software to infect the family computer
- Nearly half of teens (46%) of teens admit to downloading music or videos from a free service, which is much more likely to infect the family PC with everything from worms, viruses, ad-ware, spyware, or backdoors that allow people on the Internet to access the computer
- 16% of 16-17 year old boys have downloaded x-rated content

The Future of Internet Safety Education: Critical Lessons from Four Decades of Youth Drug Abuse Prevention

June 15, 2010

Excerpt

Publicity about online "predators" has raised considerable alarm about the extent to which Internet activities put children and adolescents at risk for sexual abuse and exploitation. More recently, concerning media stories of cyberbullying victimization and "sexting" have added to parental and community worries about the potential risks of youth technology use.

However, it is not clear what kinds of information are currently being delivered to youth and in what formats. Formal and informal programs are requested regularly by school and community leaders. A variety of presentation and classroom materials have been made available for use, with many communities developing their own materials. And the information offered to youth cover a range of topics: "Internet predators"; cyber-bullying and harassment; avoidance of pornography, violence, and hate sites; and sexual image production and distribution by youth or "sexting." Internet safety programs can include broader educational objectives as well, such as promoting youth "digital citizenship".

Unfortunately, there is no research evidence that compares the success of available programs, examines what materials or educational approaches are effective, or studies how programs are actually being implemented in communities. Outcome evaluations have been limited in sophistication and so far show no evidence that Internet safety programs reduce risky online behaviors by youth or prevent negative experiences.

Internet safety education proponents would do well to study the history of youth drug and alcohol abuse prevention, in particular. There are striking similarities in the political contexts of the two initiatives and the intensity of public concern. And there are parallels in our eagerness to prevent Internet victimization and early rushed efforts to prevent youth drug abuse in the 1970s and 80s. Internet safety proponents have a real opportunity to avoid reinventing the wheel. The remainder of the essay reviews the history of drug abuse prevention, from the large scale roll-out of Project DARE (Drug Abuse Resistance Education) in the 1980s, to the intensive efforts over the last two decades to improve youth drug abuse prevention. Critical lessons for youth Internet safety education are emphasized, with ideas about what program developers and funding agencies can do now to optimize Internet safety.

Risky Behaviors and Online Safety: A 2010 Literature Review (DRAFT)

June 2010

Excerpt

This Literature Review was produced for Harvard Berkman Center's Youth and Media Policy Working Group Initiative, co-directed by John Palfrey, Urs Gasser, and myself and funded by the MacArthur Foundation. This Literature Review builds on the 2008 LitReview that Andrew Schrock and I crafted for the Internet Safety Technical Task Force. This document is not finalized, but we want to make our draft available broadly so that scholars working in this area can inform us of anything that we might be missing.
Risky Behaviors and Online Safety: A 2010 Literature Review

It's been almost two years since the Internet Safety Technical Task Force completed its work. As a co-director of that project, I coordinated the Research Advisory Board to make certain that we included all of the different research that addressed online safety. When we shared our report, we were heavily criticized as being naive and clueless (or worse). Much of the criticism was directed at me and the researchers. We were regularly told that social network sites would radically change the picture of online safety and that we simply didn't have new enough data to understand how different things would be in a few years. Those critiques continue. As researchers who were actively collecting data and in the field, many of us are frustrated because what we see doesn't match what the politicians believe. It's been two years since we put out that first Lit Review and I'm glad to be able to share an updated one with all sorts of new data. Not surprisingly (to us at least), not much has changed.
What you'll find is that researchers have gone deeper, getting a better picture of some of the dynamics and implications. You'll also find that the overarching picture has not changed much. Many of the core messages that we shared in the ISTTF report continue to hold. In this updated Lit Review, we interrogate the core issues raised in the ISTTF report and introduce new literature that complements, conflicts, or clarifies what was previously said. We bring in international data to provide a powerful comparison, most notably from the reports that came out in the EU and Australia. And we highlight areas where new research is currently underway and where more research is necessary.

Berkman Center Sexting: Youth Practices and Legal Implications

June 22, 2010

Excerpt

This document addresses legal and practical issues related to the practice colloquially known as sexting. It was created by Harvard Law School's Cyberlaw Clinic, based at the Berkman Center for Internet & Society, for the Berkman Center's Youth and Media Policy Working Group Initiative.

This document is intended to provide background for the discussion of interventions related to sexting. It begins with a definition of sexting, and continues with overviews of research and media stories related to sexting. It then discusses the statutory and constitutional framework for child pornography and obscenity. It concludes with a description of current and pending legislation meant to address sexting.

II. Definition of Sexting
There is no consistent definition of sexting in law or research. According to the National Center for Missing and Exploited Children ("NCMEC"), the term refers to the practice of "youth writing sexually explicit messages, taking sexually explicit photos of themselves or others in their peer group, and transmitting those photos and/or messages to their peers." This definition is not intended to include "situations in which young people send sexually explicit images of themselves to adults." As NCMEC notes, however, "this distinction becomes more difficult based upon the age difference between the two parties," for example when an 18‐year‐old high school student is involved. It also is not meant to include those situations in which images are sent under "duress, coercion, blackmail, or enticement," although determining whether any of these exist in a given incident can be complicated.

III. Research on Sexting
To date, four surveys have been conducted on sexting among teens and young adults in the United States. The most recent, released by the Pew Research Center in December 2009, focuses on teens ages 12‐17 who report sending or receiving "sexually suggestive nude or nearly nude images via text messaging" on their cell phones. According to the survey, 4% of teens between the ages of 12 and 17 have sent sexually provocative images of themselves to someone else via text message, while 15% have received such images from someone they know. The Pew data indicates that older teens are much more likely to engage in such behavior, with 8% of 17‐year‐olds having sent a nude or semi‐nude image by text and 30% having received such an image.

Pew’s focus groups reveal three main scenarios in which sexting tends to occur: (1) exchanges of images solely between two romantic partners; (2) exchanges between romantic partners that are then shared with others outside the relationship; and (3) exchanges where at least one person would like to start a romantic relationship. Pew’s data suggests that sexting has become a form of “relationship currency,” with girls in particular sometimes feeling pressure to send images.

The three earlier surveys indicate higher levels of sexting involvement among teens and young people than does the Pew survey, ranging from 20 ‐ 24%. This discrepancy is likely based on two factors. First, the Pew study focuses on teens between the ages of 12 and 17, whereas the other studies focus on older teens and young adults. Second, the Pew survey asks only about nude or nearly nude images sent or received via text messaging. The other surveys are framed more broadly, asking respondents whether they have “shared” such images, “sent/posted” such images, or sent such images in “emails or text messages.”

PEW Teens and Mobile Phones

April 2010

Excerpt

Daily text messaging among American teens has shot up in the past 18 months, from 38% of teens texting friends daily in February of 2008 to 54% of teens texting daily in September 2009. And it's not just frequency – teens are sending enormous quantities of text messages a day. Half of teens send 50 or more text messages a day, or 1,500 texts a month, and one in three send more than 100 texts a day, or more than 3,000 texts a month. Older teen girls ages 14-17 lead the charge on text messaging, averaging 100 messages a day for the entire cohort. The youngest teen boys are the most resistant to texting – averaging 20 messages per day.

Text messaging has become the primary way that teens reach their friends, surpassing face-to-face contact, email, instant messaging and voice calling as the go-to daily communication tool for this age group. However, voice calling is still the preferred mode for reaching parents for most teens.

This report particularly highlights the rapid rise of text messaging in recent months. Some 72% of all U.S. teens are now text message users,8 up from 51% in 2006. Among them, the typical texter sends and receives 50 texts a day, or 1500 per month. By way of comparison, a Korean, Danish or a Norwegian teen might send 15 – 20 a day and receives as many.

Changes in subscription packages have encouraged widespread texting among U.S. teens and has made them into world class texters. As a result, teens in America have integrated texting into their everyday routines. It is a way to keep in touch with peers even while they are engaged in other social activities. Often this is done discreetly and with little fuss. In other cases, it interrupts in-person encounters or can cause dangerous situations.

To understand the role that cell phones play in teens’ lives, the Pew Research Center’s Internet & American Life Project and the University of Michigan’s Department of Communication Studies conducted a survey and focus groups in the latter part of 2009. The phone survey was conducted on landline and cell phones and included 800 youth ages 12-17 and one of their parents.

PEW Cyberbullying 2010: What the Research Tells Us

May 6, 2010

An updated look at the research and definitions around bullying and cyberbullying, this talk was presented to the Youth Online Safety Working Group assembled by National Center for Missing and Exploited Children. Amanda's talk draws upon the work of the Pew Internet Project, UNH's Crimes Against Children Research Center, the work of Internet Solutions for Kids as well as research by professors Sameer Hinduja and Justin Patchin. Amanda unpacks both what current research can tell us about cyberbullying as well as where the gaps in our understanding of this issue lie.

PEW Social Media and Young Adults

February 3, 2010

Excerpt

Two Pew Internet Project surveys of teens and adults reveal a decline in blogging among teens and young adults and a modest rise among adults 30 and older. In 2006, 28% of teens ages 12-17 and young adults ages 18-29 were bloggers, but by 2009 the numbers had dropped to 14% of teens and 15% of young adults. During the same period, the percentage of online adults over thirty who were bloggers rose from 7% blogging in 2006 to 11% in 2009.

Much of the drop in blogging among younger internet users may be attributable to changes in social network use by teens and young adults. Nearly three quarters (73%) of online teens and an equal number (72%) of young adults use social network sites. By contrast, older adults have not kept pace; some 40% of adults 30 and older use the social sites in the fall of 2009.
Additionally, teens ages 12-17 do not use Twitter in large numbers – just 8% of online teens 12-17 say they ever use Twitter, a percentage similar to the number who use virtual worlds. This puts Twitter far down the list of popular online activities for teens and stands in stark contrast to their record of being early adopters of nearly every online activity.

However, even as blogging declines among those under 30, wireless connectivity continues to rise in this age group. “We often look to younger generations to see where technology use might be headed in the future,” lead author Amanda Lenhart noted. “People under 30 have often been in the vanguard of internet and cell-phone use, and it will be interesting to see how much of their enthusiasm for new gadgets is a time-of-life issue, and how much will ripple through the broader culture in the coming years.”

NCSA Study: Too few schools are teaching cyber safety

Feb 26th, 2010

Excerpt

Students aren’t getting enough instruction in school on how to use technology and the internet in a safe and responsible manner, a new poll suggests.

Released by the National Cyber Security Alliance (NCSA) and supported by Microsoft Corp., the survey found fewer than one-fourth of U.S. teachers have spent more than six hours on any kind of professional development related to cyber ethics, safety, or security within the last 12 months.

More than half of teachers reported their school districts do not require these subjects as part of the K-12 curriculum, and only 35 percent said they've taught proper online conduct to their students.

Despite the lack of training and consistent teaching of internet safety, the survey shows that America's teachers, school administrators, and technology coordinators strongly agree that cyber ethics, safety, and security should be taught in schools.

The poll, conducted by Zogby International, surveyed more than 1,000 teachers, 400 school administrators, and 200 technology coordinators. Results were analyzed in conjunction with the Maryland-based research group Educational Technology Policy, Research, and Outreach (ETPRO).

Key findings of the survey include:

- More than 90 percent of technology coordinators, school administrators, and teachers support teaching cyber ethics, safety, and security in schools. Yet, only 35 percent of teachers and just over half of school administrators report that their school districts require the teaching of these subjects in their curriculum.
- Lessons on these topics aren't being integrated very often into everyday instructional activities. For example, only 27 percent of teachers have taught about the safe use of social networks in the past 12 months; only 18 percent have taught about online scams, fraud, and social engineering; and only 19 percent have taught about safe passwords. Overall, 32 percent of teachers said they have not taught cyber ethics, and 44 percent of teachers said they have not taught cyber safety or security.
- Teachers and administrators have different opinions as to who should be responsible for educating students about these topics. While 72 percent of teachers said parents bear the primary responsibility for teaching these topics, 51 percent of school administrators said teachers are mostly responsible.

"The study illuminates that there is no cohesive effort to [give] young people the education they need to safely and securely navigate the digital age and prepare them as digital citizens and employees," said Michael Kaiser, NCSA's executive director. "Unfortunately, we are not meeting the needs of schools, teachers, or students."

Microsoft Online Reputation in a Connected World

January, 2010

Excerpt

This research examines the expanding role of online reputation in both professional and personal lives. It studies how recruiters and HR professionals use online reputational information in their candidate review processes, and how consumers feel about this use of their information. It investigates the steps consumers take to monitor and protect their online reputation.

An online reputation is the publicly held social evaluation of a person based on his or her behavior, what he or she posts, and what others (such as individuals, groups, and Web services) share about the person on the Internet.

The Internet constitutes a worldwide database, where information is archived and not easily deleted. People, companies, and governments are increasingly using technologies such as social networking and video sharing, blogs, and search engines to create and share content with others around the world. Whether it is for a job application, friendship, dating, or other purposes, when people want to learn about someone, they turn to this ever-growing pool of information. Online reputation, therefore, plays an important role in personal and professional life and has become a significant factor in making hiring decisions.

This report summarizes online reputation research commissioned by Microsoft. It was conducted by Cross-Tab between December 10 and 23, 2009, in France, Germany, the United Kingdom, and the United States. Approximately 275 recruiters, human resources (HR) professionals, and hiring managers, and about 330 consumers interviewed in each country.

This study explores the attitudes of consumers, HR professionals, and recruiters on the subject of online reputation. In particular, it examines the impact of online reputation on hiring and how people manage their online reputation.

Highlights of the study's findings include:

- The recruiters and HR professionals surveyed are not only checking online sources to learn about potential candidates, but they also report that their companies have made online screening a formal requirement of the hiring process.
- Of U.S. recruiters and HR professionals surveyed, 70% say they have rejected candidates based on information they found online. Though not as frequently, respondents from the U.K. and Germany report the same trend.
- Recruiters and HR professionals surveyed report being very or somewhat concerned about the authenticity of the content they find.
- In all countries, recruiters and HR professionals say they believe the use of online reputational information will significantly increase over the next five years.
- Positive online reputations matter. Among U.S. recruiters and HR professionals surveyed, 85% say that positive online reputation influences their hiring decisions at least to some extent. Nearly half say that a strong online reputation influences their decisions to a great extent.
- Consumers surveyed have mixed opinions about the appropriateness of recruiters and HR professionals examining some types of online content. Most find it reasonable that recruiters and HR professionals check information on professional sites. There is greater concern, however, about recruiter scrutiny of photos, videos, and other personal content including blogs, personal social network pages, organizations they are affiliated with, financial information, and the like.
- Consumers surveyed use a variety of methods to monitor and manage the information posted about them online. Most notably, they use multiple personas, search for information about themselves, adjust privacy settings, and refrain from posting content that they believe could damage their reputation.
- Though most consumers surveyed do manage their reputation at least to some extent, there are a significant percentage of respondents (between 30% and 35% depending on nationality) who don't feel their online reputation affects either their personal or professional life. Consequently, they are not taking steps to manage their reputations.

How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?

April 14, 2010

“We suggest…that young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data.”

Media reports teem with stories of young people posting salacious photos online, writing about alcohol-fueled misdeeds on social networking sites, and publicizing other ill-considered escapades that may haunt them in the future. These anecdotes are interpreted as representing a generation-wide shift in attitude toward information privacy. Many commentators therefore claim that young people “are less concerned with maintaining privacy than older people are.” Surprisingly, though, few empirical investigations have explored the privacy attitudes of young adults. This report is among the first quantitative studies evaluating young adults’ attitudes. It demonstrates that the picture is more nuanced than portrayed in the popular media.

In this telephonic (wireline and wireless) survey of internet using Americans, we found that large percentages of young adults (those 18-24 years) are in harmony with older Americans regarding concerns about online privacy, norms, and policy suggestions. In several cases, there are no statistically significant differences between young adults and older age categories on these topics. Where there were differences, over half of the young adult-respondents did answer in the direction of older adults. There clearly is social significance in that large numbers of young adults agree with older Americans on issues of information privacy.

A gap in privacy knowledge provides one explanation for the apparent license with which the young behave online. 42 percent of young Americans answered all of our five online privacy questions incorrectly. 88 percent answered only two or fewer correctly. The problem is even more pronounced when presented with offline privacy issues – post hoc analysis showed that young Americans were more likely to answer no questions correctly than any other age group.

PEW Reputation Management and Social Media

May 26, 2010

More than half (57%) of adult internet users say they have used a search engine to look up their name and see what information was available about them online, up from 47% who did so in 2006. Young adults, far from being indifferent about their digital footprints, are the most active online reputation managers in several dimensions. For example, more than two-thirds (71%) of social networking users ages 18-29 have changed the privacy settings on their profile to limit what they share with others online.

Reputation management has now become a defining feature of online life for many internet users, especially the young. While some internet users are careful to project themselves online in a way that suits specific audiences, other internet users embrace an open approach to sharing information about themselves and do not take steps to restrict what they share.

“Search engines and social media sites now play a central role in building one’s identity online,” said Mary Madden, Senior Research Specialist and lead author of the report, “Many users are learning and refining their approach as they go–changing privacy settings on profiles, customizing who can see certain updates and deleting unwanted information about them that appears online.”

When compared with older users, young adults are more likely to restrict what they share and whom they share it with. “Contrary to the popular perception that younger users embrace a laissez-faire attitude about their online reputations, young adults are often more vigilant than older adults when it comes to managing their online identities," said Madden.

Yahoo: Child Safety Study

June 10, 2010

Excerpt

Yahoo has released some findings from a survey about how parents monitor children's online behavior. The company says it makes safety a company priority by supporting efforts to educate children, parents, adults, and communities about safe online experiences. Yahoo takes a "multi-faceted approach in promoting a safer online experience," Yahoo spokesperson Terrell Karlsten tells WebProNews.

"Staying safe online is not a one-time conversation with children, it's an ongoing process that parents and youth need to be aware of every time they log on," adds Karlsten.

The survey (conducted among 2,003 Internet users in the U.S., ages 18–64) found that parents are taking action, but cyber-bullying education is needed. Stats include:

- 78% of parents are concerned about their children's online safety.

- 70% of parents talk to their children about online safety at least 2-3 times a year; 45% talk to their children at least once a month.

- 74% of parents are connected to their children's profiles on social networking sites.

- 71% of parents have taken at least one action to manage their children's use of the Internet or cell phones such as checking to see where children are searching online, setting time limits for children's use of computers or cell phones, setting parental controls on video sites, and using filters to limit where children go on the Web.

- 81% of parents know what cyberbullying is.

- 25% who are aware of cyberbullying have either been victims or know someone else affected by cyberbullying.

- 37% of parents feel that they know what to do about cyberbullying.

- 73% want their child's school to play an active role in teaching kids about online safety and citizenship.

- 71% of dads (compared to 63% of moms) say they are taking at least one action to help manage their children's online behavior including having conversations about respecting the privacy of others and checking their children's privacy settings. More dads than moms have had a conversation with their children about their digital reputations and how to promote a positive online reputation.

- 53% of dads said they plug their children's names into a search engine at least 2–3 times per year (compared to 38% of moms) – 33% of dads said they do this search at least once a month.

- 47% of dads have conversations about online safety at least once a month, compared to 42% of moms.

- According to the survey, more dads than moms use filters to limit where their kids go online, and more dads monitor the time children send text messages and how many text messages they send.

Norton Online Family Report Global insights into family life online

June 10, 2010

Excerpt

The **Norton Online Family Report** examines children's online behavior and experiences compared with parents' knowledge and understanding of these. It highlights key contrasts and disconnects between parents and their children and offers advice and guidance for parents on how to bridge the gaps.

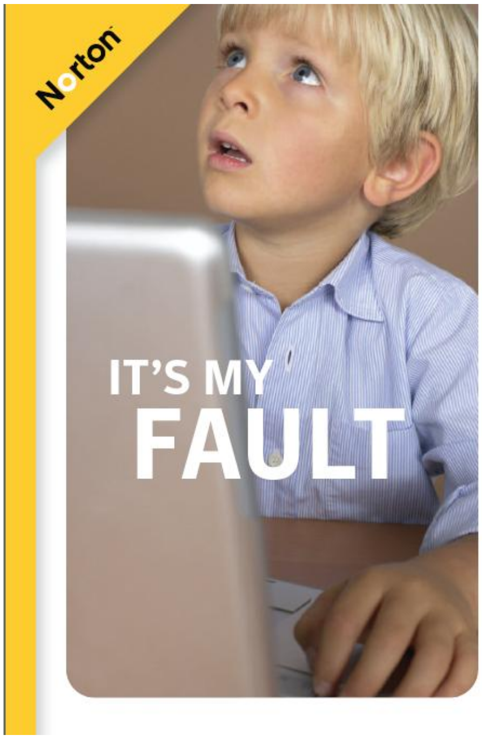
The Report finds that children are spending an increasing amount of time online, and in general parents are aware of this and have a fair idea of the main activities their children participate in online. Parents are concerned about children accessing indecent material or giving out personal information online, yet they underestimate the extent to which children download games, music and video. These are key activities which may expose children to inappropriate content and encourage them to disclose their personal details.

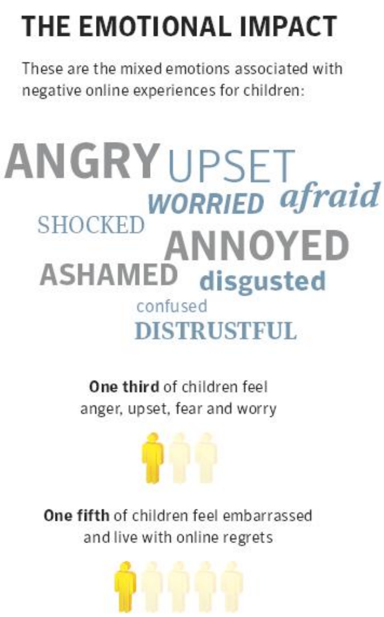
The perceived need for parents to control children's online activities varies hugely. In Canada and the US, **six in 10 adults** think parents should have **full control** over everything their child does online. In Italy and China, however, parents are more likely to believe in **empowering** their children to make the right decisions.

One of the most surprising insights from the Report is parents' lack of awareness about the extent of children's negative experiences online. Almost **two thirds** of children have had a negative experience online, whereas only **45%** of parents realize this. Children take an enormous sense of responsibility for their negative experiences online, perhaps without justification. They report feelings of anger, being upset and fear when they encounter an unpleasant situation.

The **good news** is that children actually want more parental involvement in their online lives. The majority state they would like to turn to their parents for support and advice when things go wrong. Children understand that ethical behavior is as important online as it is offline and are setting their own rules for acceptable online behavior. Children's own rules include not bullying or harassing people online, not passing on embarrassing photos or posts about others, telling parents if they or others are being bullied, and not saying or doing things online that they wouldn't do in an offline world.

There is clearly an important role for parents to play by increasing their understanding of the Internet, the role it plays in their children's lives, and the experiences their children are having online. Children need 'parenting' online as much as they do in their offline lives, and they would welcome more parental involvement.



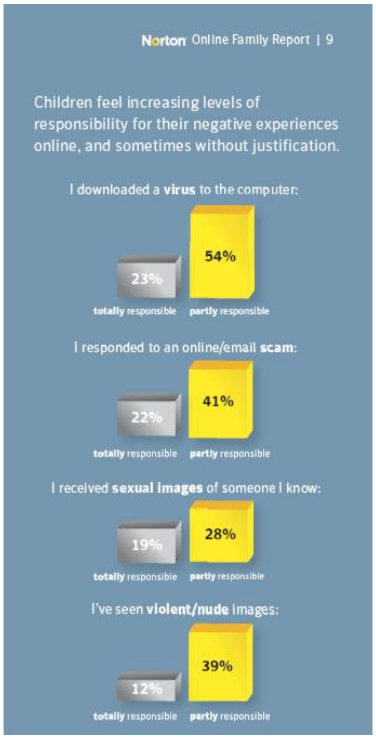

THE EMOTIONAL IMPACT

These are the mixed emotions associated with negative online experiences for children:

ANGRY UPSET
WORRIED afraid
SHOCKED
ANNOYED
ASHAMED disgusted
confused
DISTRUSTFUL

One third of children feel anger, upset, fear and worry

One fifth of children feel embarrassed and live with online regrets



Children feel increasing levels of responsibility for their negative experiences online, and sometimes without justification.

Youth Safety on a Living Internet:

June 4, 2010

Excerpt

The Online Safety and Technology Working Group, formed one year ago as an outcome of the ”Protecting Children in the 21st Century” Act. This groups mission was to review industry efforts and provide recommendations that would increase child safety online through education, labeling and family safety technologies.

This group has now released their 148 page report: Youth Safety on a living internet which represents a solid amount of work by highly respected individuals in their fields – which makes it all the more frustrating that there isn’t at least one recommendation that we haven’t heard before. The report is an excellent study of where we’ve been, and even where we are. In the reports own words, “Any report about both the Internet and children is necessarily a freeze frame of a rapidly moving landscape”. But what’s missing is an innovative vision that sculpts a safer future. Reiterating the same recommendations is likely to produce the same result.

Summary: SUBCOMMITTEE ON INTERNET SAFETY EDUCATION

Recommendations

1. Keep up with the youth-risk and social-media research, and create a web-based clearinghouse that makes this research accessible to all involved with online safety education at local, state, and federal levels.
2. Coordinate Federal Government educational efforts.
3. Provide targeted online-safety messaging and treatment.
4. Avoid scare tactics and promote the social-norms approach to risk prevention.
5. Promote digital citizenship in pre-K-12 education as a national priority.
6. Promote instruction in digital media literacy and computer security in pre-K-12 education nationwide.
7. Create a Digital Literacy Corps for schools and communities nationwide.
8. Make evaluation a component of all federal and federally funded online safety education programs (evaluation involving risk-prevention expertise).
9. Establish industry best practices.
10. Encourage full, safe use of digital media in schools' regular instruction and professional development in their use as a high priority for educators nationwide.
11. Respect young people's expertise and get them involved in risk-prevention education.
12.

Summary: SUBCOMMITTEE ON PARENTAL CONTROLS & CHILD PROTECTION TECHNOLOGY

Recommendations

1. Engage in ongoing awareness-building efforts.
2. Promote greater transparency for parents as to what sort of content and information will be accessible and recorded with a given product when their children are online.
3. Bake parental empowerment technologies and options possible into product development whenever possible.
4. Develop a common set of terms, agreed upon by the industry, across similar technologies.
5. Promote community reporting and policing on sites that host user-generated content.

Summary: SUBCOMMITTEE ON CHILD PORNOGRAPHY REPORTING

Recommendations

1. Task the appropriate executive agency with the objective to conduct a survey using an empirically reliable method to assess industry efforts to promote online safety by means of the new reporting provisions of § 2258A.
2. Encourage outreach by NCMEC, government agencies, advocacy groups, and service providers to promote increased awareness of the PROTECT Our Children Act through education, information sharing efforts, and the establishment of sound practices for reporting and data preservation.
3. Encourage nascent or smaller service providers who may lack the necessary networking contacts or experience to seek out meetings with NCMEC and law enforcement concerning the reporting and preservation provisions of the Act.
4. Continue to encourage collaboration and information sharing among providers to develop new technologies that disrupt the transfer of online child pornography and facilitate reporting to NCMEC.
5. Consider tax credits or other financial incentives to assist service providers in bearing the development and implementation costs associated with securely retaining data outside the course of normal business.
6. Consider incentives for service providers to establish wellness programs for the employees who face the task of reviewing disturbing images of child sexual abuse in order to maintain compliance with the mandatory reporting requirements.

Summary: SUBCOMMITTEE ON DATA RETENTION

Recommendations

1. ISPs and OSPs should have regular meetings and engage ICAC task forces and federal law enforcement agencies to cross-train on emerging threats, resolve operational glitches, and develop a set of evolving practices and procedures.
2. Privacy concerns regarding vast amounts of stored data must be addressed.
3. If they are to occur, data retention debates should happen at the federal level, so as not to add further confusion concerning competing regulations among states.
4. Congress should assess the results of the data preservation procedures enacted in the PROTECT Our Children Act before considering mandatory data retention.
5. We encourage you to read the full subcommittee reports contained in this document to grasp fully not only the insight contained in them, but also the twenty-six (26) recommendations we have provided.

Cyberbullying Research Summary: Cyberbullying and Suicide

Excerpt

Youth suicide continues to be a significant public health concern in the United States. Even though suicide rates have decreased 28.5 percent among people in recent years, upward trends were identified in the 10- to 19-year-old age group. In addition to those who successfully end their life, many other adolescents strongly think about and even attempt suicide.

One Factor that has been linked to suicidal ideation is experience with bullying. That is, youth who are bullied, o bully others, are at an elevated risk for suicidal thoughts, attempts, and completed suicides. The reality of these links has been strengthened through research showing how experience with peer harassment (most often as a target but also as a perpetrator) contributes to depression, decreased self-worth, hopelessness, and loneliness – all of which are precursors to suicidal thoughts and behavior.

Without question, the nature of adolescent peer aggression has evolved due to the proliferation of information and communications technology. There have been several high-profile cases involving teenagers taking their own lives in part because of being harassed and mistreated over the Internet,7-9 a phenomenon we have termed *cyberbullicide* – suicide indirectly or directly influenced by experiences with online aggression.10 While these incidents are isolated and do not represent the norm, their gravity demands deeper inquiry and understanding. Much research has been conducted to determine the relationship between *traditional* bullying and suicidal ideation, and it can be said with confidence that a strong relationship exists.11, 12 Based on what we found in the extant literature base, we sought to determine if suicidal ideation was also linked to experiences with *cyberbullying* among offenders and targets.

Highlights from the Research:

- 20% of respondents reported seriously thinking about attempting suicide
- All forms of bullying were significantly associated with increases in suicidal ideation
- Cyberbullying victims were almost twice as likely to have attempted suicide compared to youth who had not experienced cyberbullying

The School Bully in Cyberspace

Teens live highly digital and media-rich lives with more communications choices than ever before. The media explosion is influencing our youths in ways never imagined. According to the 2007 Pew Internet & American Life Project report *Teens and Social Media,* by Amanda Lenhart, Mary Madden, Alexandra Rankin Macgill and Aaron Smith, most teens spend time online, and about 50 percent of those who use the Internet have at least one profile on at least one social networking Web site.

Youths use such sites to stay in touch with friends and make new ones. The Pew findings note that 28 percent of teens using the Internet maintain a blog to write about their lives, ideas, goals and dreams; to post photos; and to create and share videos. In addition, the report states that 80 percent of teens own at least one form of what is defined as "new" media technology—a cell phone, personal data assistant, or computer with Internet access.

As noted in a 2007 special supplement to the *Journal of Adolescent Health* on electronic media, the explosion of technology and its use by adolescents has many potential benefits. Technology provides a way for young people to communicate regularly with family and friends and may result in teens feeling more connected to others. "The
Internet provides opportunities for adolescents who have difficulty making friends, e.g., home-schooled or socially anxious youth, to make rewarding social connections," point out Corinne David-Ferdon and Marci Feldman Hertz in the guest editors' commentary "Electronic Media, Violence, and Adolescents: An Emerging Public Health Problem."

Home Broadband 2010

After several years of double digit growth, broadband adoption slowed dramatically in 2010. African-Americans experienced broadband adoption growth in 2010 well above the national average

After several consecutive years of modest but consistent growth, broadband adoption slowed dramatically in 2010. Two-thirds of American adults (66%) currently use a high-speed internet connection at home, a figure that is not statistically different from what The Pew Research Center's Internet & American Life Project found at a similar point in 2009, when 63% of Americans were broadband adopters.

The lack of growth in broadband adoption at the national level was mirrored across a range of demographic groups, with African-Americans being a major exception. Broadband adoption by African-Americans now stands at 56%, up from 46% at a similar point in 2009. That works out to a 22% year-over-year growth rate, well above the national average and by far the highest growth rate of any major demographic group. Over the last year, the broadband adoption gap between blacks and whites has been cut nearly in half:

- In 2009 65% of whites and 46% of African-Americans were broadband users (a 19-point gap)
- In 2010 67% of whites and 56% of African-Americans are broadband users (an 11-point gap)

By a 53%-41% margin, Americans say they do not believe that the spread of affordable broadband should be a major government priority. Contrary to what some might suspect, non-internet users are *less likely than* current users to say the government should place a high priority on the spread of high-speed connections.

In this survey, Americans were asked: "Do you think that expanding affordable high-speed internet access to everyone in the country should be a top priority for the federal government, important but a lower priority, not too important, or should it not be done?" The majority chose the last two options:

- 26% of Americans say that expansion of affordable broadband access should not be attempted by government.

- 27% said it was “not too important” a priority

- 30% said it was an important priority.

- 11% said it should be a top priority.

Those who are not currently online are especially resistant to government efforts to expand broadband access. Fully 45% of non-users say government should not attempt to make affordable broadband available to everyone, while just 5% of those who don’t use the internet say broadband access should be a top federal government priority. Younger users (those under age 30) and African-Americans were the most likely to favor expanded government efforts towards broadband access, while older Americans were among the least likely to back the expansion of affordable broadband access as a government priority.

Generation M^2 Media in the Lives of 8 to 18 year-olds

Understanding the role of media in young people’s lives is essential for those concerned about promoting the healthy development of children and adolescents, including parents, pediatricians, policymakers, children’s advocates, educators, and public health groups. It is the purpose of this study to foster that understanding by providing data about young people’s media use: which media they use, which they own, how much time they spend with each medium, which activities they engage in, how often they multitask, and how they differ from one another in the patterns of their media use. Our aim is to provide a more solid base from which to examine media’s effects on children and to help guide those who are proactively using media to inform and educate America’s youth.

The study is one of the largest and most comprehensive publicly available sources of information on the amount and nature of media use among American youth:

- It includes a large national sample of more than 2,000 young people from across the country;
- It covers children from ages 8 to18, to track changes from childhood through the transitional “tween” period, and on into the teenage years;
- It explores a comprehensive array of media, including TV, computers, video games, music, print, cell phones, and movies;
- It is one of the only studies to measure and account for media multitasking—the time young people spend using more than one medium concurrently; and
- It gathers highly detailed information about young people’s media behavior, including responses to an extensive written questionnaire completed by the entire sample, plus results from a subsample of approximately 700 respondents who also maintained week-long diaries recording their media use in half-hour increments.

Finally, because this is the third wave of the Kaiser Family Foundation’s studies of children’s media use, it not only provides a detailed look at current media use patterns among young people, but also documents changes in children’s media habits since the first two waves of the study, in 1999 and 2004.

McAfee Threats Report: Second Quarter 2010

This edition of the *McAfee Threats Report* examines the second quarter of 2010 and finds some very different results compared with previous quarters. Last quarter we saw a leveling off in some threat vectors while in others we saw some new developments. This quarter we find malware has resumed its usual rapid growth while the increase in spam has slowed. We see some very interesting geographical breakdowns for spam and botnets that we have not seen before. More threats have become specific and unique to those victims, both corporate and consumer, in different parts of the world.

This quarter we also see the global breakdown of malware to be quite different from that of previous quarters. From January to March we found the top malware to be the same around the world, a phenomenon we had not observed previously; but this quarter's breakdown shows specific threats tend to plague specific regions. We look very closely at growth trends for fake-alert software, password stealing Trojans, social networking malware such as Koobface, as well as malware that abuses USB and other storage devices.

We examine event and keyword abuse through search engines as well as which vulnerabilities were most frequently exploited throughout the quarter. It should come as no surprise that events such as the FIFA World Cup in South Africa and incidents in the Middle East were highly abused by both cybercriminals and political hacktivists. Remember: the bad guys read the same news as we do. We report on web and network threats such as phishing and malicious website growth and see what parts of the world are engaging in the most SQL-injection attacks.

We finish with an overview of the quarter's most interesting incidents in both cybercrime and hactivism. We hope you find this edition of the *McAfee Threats Report* instructive.

Privacy Online: Fair Information Practices in the Electronic Marketplace

The Federal Trade Commission has been studying online privacy issues since 1995. This is the Commission's third report to Congress examining the state of online privacy and the efficacy of industry self-regulation. It presents the results of the Commission's 2000 Online Privacy Survey, which reviewed the nature and substance of U.S. commercial Web sites. privacy disclosures, and assesses the effectiveness of self-regulation.

The Report also considers the recommendations of the Commission-appointed Advisory Committee on Online Access and Security. Finally, the Report sets forth the Commission's conclusion that legislation is necessary to ensure further implementation of fair information practices online and recommends the framework for such legislation.

In its 1998 report, *Privacy Online: A Report to Congress* (.1998 Report.), the Commission described the widely-accepted fair information practice principles of *Notice*, *Choice*, *Access,* and *Security*. The Commission also identified *Enforcement* . the use of a reliable mechanism to provide sanctions for noncompliance . as a critical component of any governmental or self-regulatory program to protect privacy online. In addition, the 1998 Report presented the results of the Commission's first online privacy survey of commercial Web sites. While almost all Web sites (92% of the comprehensive random sample) were collecting great amounts of personal information from consumers, few (14%) disclosed anything at all about their information practices.

Prepared Statement of the Federal Trade Commission on Consumer Privacy

Privacy has been central to the Commission's consumer protection mission for more than a decade. Over the years, the Commission has employed a variety of strategies to protect consumer privacy, including law enforcement, regulation, outreach to consumers and businesses, and policy initiatives.2 In 2006, recognizing the increasing importance of privacy to consumers and a healthy marketplace, the FTC established the Division of Privacy and Identity Protection, which is devoted exclusively to privacy-related issues.3

Although the FTC's commitment to consumer privacy has remained constant, its policy approaches have evolved over time. This testimony describes the Commission's efforts to protect consumer privacy over the past two decades, including its two main policy approaches: (1) promoting the fair information practices of notice, choice, access, and security (the "FTC Fair Information Practices approach"); and (2) protecting consumers from specific and tangible privacy harms (the "harm-based approach"). It then discusses recent developments, including the FTC staff's Privacy Roundtables project – a major initiative to re-examine traditional approaches to privacy protection in light of new technologies and business models. It concludes by offering general comments on both Chairman Rush's and Chairman Boucher's proposed privacy legislation.

I. The FTC's Efforts to Protect Consumer Privacy

The FTC has a long track record of protecting consumer privacy. The Commission's early work on privacy issues dates back to its initial implementation in 1970 of the Fair Credit Reporting Act ("FCRA"),4 which includes provisions to promote the accuracy of credit reporting information and protect the privacy of that information. With the emergence of the Internet and the growth of electronic commerce beginning in the mid-1990s, the FTC expanded its focus to include online privacy issues. Since then, both online and offline privacy issues have been at the forefront of the Commission's agenda, as discussed in greater detail below.

A. The FTC's Fair Information Practices Approach

Beginning in the mid-1990s, the FTC began addressing consumer concerns about the privacy of personal information provided in connection with online transactions. The Commission developed an approach by building on earlier initiatives outlining the "Fair Information Practice Principles," which embodied the important underlying concepts of transparency, consumer autonomy, and accountability. In developing its approach, the FTC reviewed a series of reports, guidelines, and model codes regarding privacy practices issued since the mid-1970s by government agencies in the United States, Canada, and Europe.

From this work, the FTC identified four widely accepted principles as the basis of its own Fair Information Practices approach: (1) businesses should provide **notice** of what information they collect from consumers and how they use it; (2) consumers should be given **choices** about how information collected from them may be used; (3) consumers should be able to **access** data collected about them; and (4) businesses should take reasonable steps to ensure the **security** of the information they collect from consumers. The Commission also identified **enforcement** – the use of a reliable mechanism to impose sanctions for noncompliance with the fair information principles – as a critical component of any self-regulatory program to ensure privacy online.

To evaluate industry's compliance with these principles, the Commission examined website information practices and disclosures; conducted surveys of online privacy policies, commented on self-regulatory efforts, and issued reports to Congress. In 2000, the Commission reported to Congress that, although there had been improvement in industry self-regulatory efforts to develop and post privacy policies online, approximately one-quarter of the privacy policies surveyed addressed the four fair information practice principles of notice, choice, access, and security.7 A majority of the Commission concluded that legislation requiring online businesses to comply with these principles, in conjunction with self-regulation, would allow the electronic marketplace to reach its full potential and give consumers the confidence they need to participate fully in that marketplace.