

# OFFICIAL REPORT

ATTORNEY GENERAL BOB McDONNELL



## YOUTH INTERNET SAFETY TASK FORCE

*Released: December 20, 2006*



December 20, 2006

*Dear Youth Internet Safety Task Force Member:*

*Thank you for your six months of faithful service to the Commonwealth on the Youth Internet Safety Task Force. We all recognize that the Internet has revolutionized our lives and the way we communicate, educate and conduct business. But here in the Internet capital of the world, Virginia, we must do everything possible to protect the Internet from child pornographers, sexual predators, identity thieves and other criminals.*

*I am pleased to present the Report based on our five meetings together throughout Virginia and the work you have contributed individually and in working groups. At each of these meetings we heard from authorities in the areas of Law Enforcement, Technology, and Education. We also heard from concerned citizens, child advocacy groups, and some parents of victims about their experiences with Internet safety.*

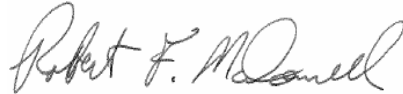
*Each of you brought to the Task Force your own particular skills and experience. Our roundtable discussions and the work we accomplished in the three different working groups that focused on Law Enforcement, Technology and Parents and Education issues produced a number of excellent recommendations. Without the collective wisdom the membership, we would not have assembled so many productive and practical ideas. These ideas will form the basis of constructive legislation that I will present to the 2007 General Assembly and some ongoing programs we will implement to improve Internet safety awareness among parents, educators and children.*

*As United States Attorney General Alberto Gonzales said: "Down to every last parent, teacher and mentor in America, we all must do our part to ensure that the Internet is not turned against our children through the evils of sexual enticement, abuse and child pornography." You have formulated innovative, practical ways to combat the problems of Internet Safety. Your recommendation of stronger sentences will address the disparity in punishments meted out across Virginia to defendants convicted of producing child pornography and soliciting minors online. Your recommendation of a statewide Advisory Committee to steer a multi-media campaign on Internet safety will increase the awareness of parents and youth about the dangers*

*posed by Internet predators. You have also identified ways to overcome the challenges of law enforcement in quickly obtaining the technical evidence necessary to prosecute child pornography and exploitation cases. These ideas, and your thoughtful recommendations are an important contribution to the public policy of Virginia and will ensure Virginia remains a safe Digital Dominion.*

*Thank you for your dedicated efforts.*

Very truly yours,

A handwritten signature in cursive script that reads "Robert F. McDonnell". The signature is written in black ink and is positioned above the printed name.

Robert F. McDonnell

## Table of Contents

Task Force on Youth Internet Safety – Full Membership.....	2
Charge of the Attorney General to the Youth Internet Safety Task Force.....	3
The State of Youth Internet Safety today.....	5
History of the Attorney General’s Youth Internet Safety Task Force .....	18
Task Force Working Group Assignment.....	20
Synopses of the Task Force meetings.....	23
Findings of the Law Enforcement Working Group .....	27
Findings of the Technology Working Group.....	48
Findings of the Parent/Education Working Group .....	59
Recommendations of the Youth Internet Safety Task Force.....	64
Conclusion .....	69
Appendix *A* - Links and Resources for Parents and Educators.....	70
Appendix *B* - Inventory of Tools and Resources for Internet Safety.....	82

## Staff of the Office of Attorney General

Robert F. McDonnell, Attorney General of the Commonwealth of Virginia  
Richard B. Campbell, Deputy, Technology, Real Estate, Environmental and  
Transportation Division  
Lisa M. Hicks-Thomas, Section Chief, Computer Crime Section  
Russell E. McGuire, Assistant Attorney General, Computer Crime Section, Staff  
Attorney  
Samuel E. Fishel, Assistant Attorney General, Computer Crime Section, Staff Attorney  
Matthew D. Nelson, Assistant Attorney General, Computer Crime Section, Staff  
Attorney  
Thomas A. Garrett, Jr., Assistant Attorney General, Computer Crime Section  
Les Lauziere, Criminal Investigator, Computer Crime Section  
Patrice Sandridge, Criminal Investigator, Computer Crime Section  
George McLaughlin, Criminal Investigator, Computer Crime Section  
Jan Myer, Administrative Legal Secretary Senior, Computer Crime Section  
Corrine Vaughn, Director, Victim Notification Program  
Donna Creekmore, Legal Secretary Senior, Transportation Section

## Task Force Members

Honorable Eileen M. Addison, Comm. Attorney York County and City of Poquoson  
Elizabeth Banker, Associate General Counsel, Yahoo!  
Dr. Sally K. Boese, Virginia Association of Independent Schools  
Kenneth and Mary Alice Booth, Concerned Parents  
Elisabeth A. Bresee, Vice President, Capital One  
Honorable Mike Brown, Sheriff, Bedford County Sheriff's Office  
John L. Brownlee, United States Attorney, Western District of Virginia  
Dr. Billy Cannaday, Jr., Superintendent of Public Instruction, Virginia Department of Education  
Michelle Collins, National Center for Missing and Exploited Children  
Charles D. Curran, Chief Counsel, Policy & Regulatory, American Online  
Liz Eraker, Policy Analyst, Google, Inc.  
Colonel W. Steve Flaherty, Superintendent, Department of State Police  
Dianne Florence, President, Virginia PTA  
David Foster, Arlington School Board  
Anne Gavin, State Government Affairs Regional Manager, Microsoft Corporation  
Robert E. Gwaltney, Assistant Special Agent in Charge, FBI Richmond  
Honorable Michael N. Herring, Commonwealth's Attorney City of Richmond  
James L. Hilton, Chief Information Officer, University of Virginia  
Honorable Janet D. Howell, Senate of Virginia  
Honorable Robert Hurt, House of Delegates of Virginia  
Virginia James, Cox High School  
Bobbie Kilberg, President & CEO, Northern Virginia Technology Council  
Rick Lally, President, Hampton Roads Technology Council  
Ray LaMura, President, Virginia Cable Telecommunication Association  
Rick Lane, Vice President, Government Affairs, News Corporation  
Honorable Ryan T. McDougale, Senate of Virginia  
Col. Rodney D. Monroe, Chief, Richmond Police Department  
Officer Stan Moorefield, C.C.P.S., Virginia Association of School Resource Officers  
Honorable Mark D. Obenshain, Senate of Virginia  
William A. Pusey, Jr., Concerned Home School Parent  
Thomas M. (Tommy) Quigley, Jr., Virginia High School Student  
Donna Rice Hughes, Enough is Enough  
Chuck Rosenberg, United States Attorney, Eastern District of Virginia  
John Ryan, Vice President and Chief Counsel, America Online  
Dr. Steve Shelby, West End Presbyterian Church  
Honorable Kim Slayton-White, Commonwealth's Attorney Halifax County  
Carter Slough, Virginia High School Student  
Robert J. Stolle, Executive Director, Greater Richmond Technology Council  
Mr. John Titus, Principal, James River High School  
Rosemary Tribble, Community Leader  
Joel Wiginton, Vice President & Senior Counsel, Government Affairs, Sony

## ***Charge of the Attorney General to the Youth Internet Safety Task Force***

Portions of the following charge are excerpted from Attorney General McDonnell's address to the Youth Internet Safety Task Force on July 14, 2006 at the National Center for Missing and Exploited Children in Alexandria, Virginia:

This is quite a lineup of folks who are leaders in law enforcement, education, the technology community, and concerned parents who are focused on this one mission. I am honored that all of you have agreed to serve because it takes the leadership of people at all levels in order to craft a policy that will achieve success.

The Internet has become an agent of revolution not only in Virginia but around the world. It has been a mechanism for information exchange for communication, for electronic commerce, and has changed the way we conduct business. It has ushered in a new series of commercial and public safety concerns that policymakers need to address. That is why this is such a timely and important topic.

Why is this important to Virginia? The estimates are anywhere from 40-50% of the world's Internet traffic goes through Northern Virginia. This is the information technology revolution epicenter. It is smart government for Virginia to do everything to protect the Internet to ensure that it stays the great agent of change and information, communication, electronic commerce, but not the safe haven of criminals. That is our challenge. To find ways to improve safety, particularly for children on the Internet, without hurting commercial or constitutional rights. That is our mission as we go forward over these next six months.

The Internet is the new or the last frontier for child predators. Virginia has the best laws in the country dealing with sexual predators. In terms of online sexual predators, child pornographers, and identity thieves, we have only begun. This is an international problem. Child pornography might be produced in Africa or South America and transmitted into the living rooms here in Alexandria. There is so much more that needs to be done that we thought it was critically important to put together this task force of experts in various fields. I am also delighted to see our federal partners here, on the law enforcement side, because we need partners at every level of government to look at this problem.

So it is not only a focus in Virginia, but also it is a national focus for the United States Attorney General to review ways to improve Internet safety. Seventy-nine percent of Americans go online. Attorney General Gonzales estimates that more than 20,000 images of child pornography are posted on the Internet each week in the United States. The sexual exploitation of children on the Internet is a \$20 billion industry. It continues to expand in the United States. General Gonzales has indicated there are as many as 50,000 sexual predators that are trolling online for child sex victims at any given time. This is a staggering figure and I am sure we have our fair share in Virginia. The numbers are somewhat chilling. Here is the really difficult part: Only one in four will actually report the fact that they have been exposed to pornography or online

sexual exploitation to a parent or law enforcement. Most of this problem is happening under the radar screen.

We must find ways during the next six months to dramatically improve that number so that these criminal activities can be reported or prevented. A North Carolina study indicated that 71% of convicted child pornography offenders admitted molestation of a significant number of children without detection and this is another indication of how much this problem remains underground. The link between pornography and actual acting out of solicitation over the Internet and subsequent attacks on children is beyond dispute.

The Internet has created unprecedented opportunities for commerce, information, and communication, but it is also the new playing field for child predators and identity thieves. I am challenging this group to seize the opportunity to do something positive. The Attorney General's office has an active role as we are tasked by statute to have a Computer Crime Unit. We work with local and federal prosecutors around the state and prosecute computer crimes and crimes against children and identity theft, all of those via the Internet. We also have a program we take into schools all over the state and tell kids and educators a little bit about the scope of the problem and how they can protect themselves.

When you and I were growing up, we were told "don't talk to strangers" and "don't get in a car." We all listened. Now, we must take that warning and translate it to cyberspace. That is the challenge that we have. That is the challenge we will meet. Thank you for your service.

# THE STATE OF YOUTH INTERNET SAFETY IN VIRGINIA

## **BACKGROUND**

The Internet has revolutionized society. Its impact permeates almost every aspect of our lives. For young people, the Internet is an efficient educational tool, a forum to communicate with people around the world and a place to play games and have fun.

Unfortunately, there is a dark side to the Internet. Online predators use it to expose children and teenagers to various forms of offensive and threatening behavior, including unwanted sexual material and sexual solicitations. The sexual exploitation of children on the Internet is a \$20 billion industry that continues to expand in the United States and abroad.<sup>1</sup> Recently, United States Attorney General Alberto Gonzales declared: “There are as many as 50,000 predators online trolling for child sex victims at any given time.”

According to the United States Department of Justice, *one in five children, 10-17 years old, receive an unwanted sexual solicitation online.*<sup>2</sup> The Crimes Against Children Research Center reports that *one in thirty-three children, ten to seventeen years old, receive an aggressive sexual solicitation, and one in four ten to seventeen year olds had an unwanted exposure to pictures of naked people or people having sex.*<sup>3</sup>

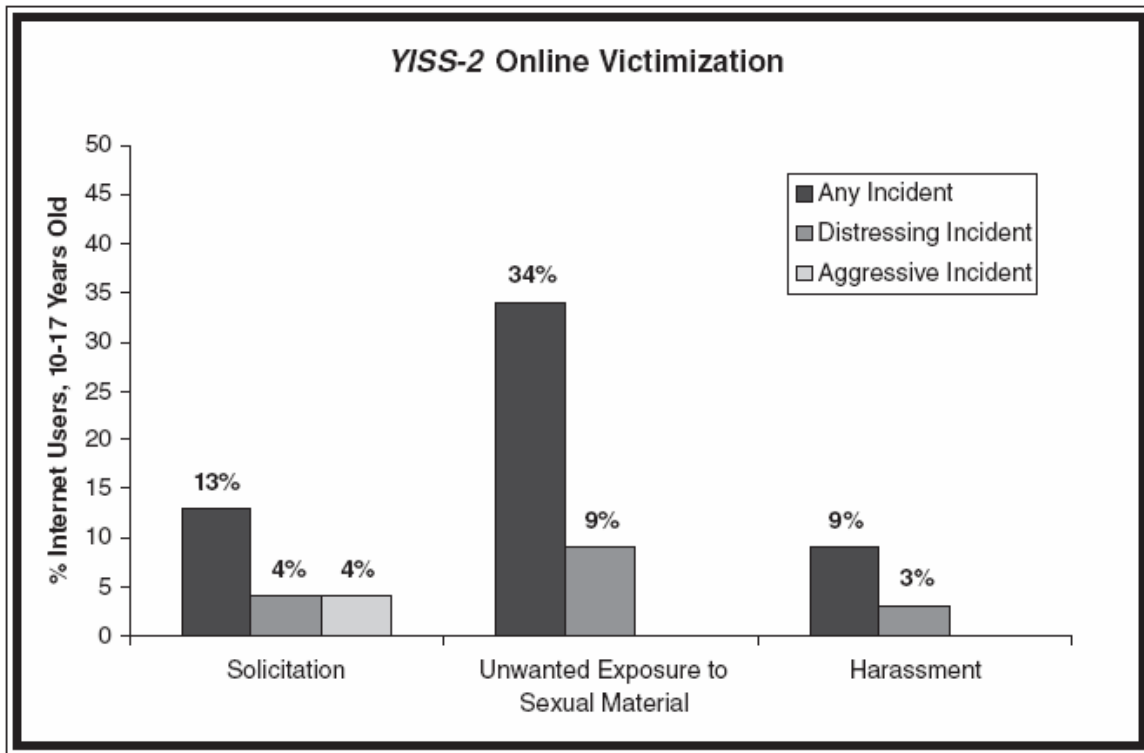
---

<sup>1</sup> Joshua Brockman, *Child Sex as Internet Fare, Through Eyes of a Victim*, N.Y. Times, (April 5, 2006).

<sup>2</sup> *Highlights of the Youth Internet Safety Survey*, United States Department of Justice (2006).

<sup>3</sup> Crimes Against Children Research Center, *Online Victimization: A Report on the Nation's Youth* (June, 2000).

Children face numerous threats over the Internet. A recent Youth Internet Safety Study (YISS-2) polled a representative sample of children ages 10-17 to determine the percentage of children who are exposed to criminal activity. The following graph, drawn from the study, depicts trends of three common dangers that children face online and the percentage of children affected<sup>4</sup>:



The children of Virginia are not immune to Internet predation. Several highly publicized cases illustrate this point. In 2006, 38-year-old Gregory J. Mitchel pleaded guilty in United States District Court in Roanoke to four felonies including production, sale, distribution, and possession of child pornography.<sup>5</sup> Mitchel began cultivating a relationship with his victim, Justin Berry, through instant messaging when Justin was 16. Mitchel used the Internet to victimize Justin, persuading him to perform sex acts in

<sup>4</sup> J. Wolak, D. Finkelhor and K. Mitchell, *Online Victimization of Youth, Five Years Later*, p.16, (2005).

<sup>5</sup> Kurt Eichenwald, *Virginia Man Pleads Guilty in Online Pornography Case*, *N.Y. Times*, (January 29, 2006).

front of a web-cam. The relationship lasted several years during which Mitchel traveled to Mexico to meet Justin and molest him.

In 2004, Kelly Karl Bowen pleaded guilty to forcible sodomy, production of child pornography, and online solicitation of children. Bowen was a Portsmouth elementary school teacher who abused his position of authority and victimized his students over the Internet. In December 2004, David Woolard of Richmond pleaded guilty to two counts of online solicitation. Woolard was a former Governor's school teacher who attempted to cultivate a sexual relationship online with a teenager whom he had known several years prior. In 2005, a Richmond jury found Michael Bodine guilty of possession and reproduction of child pornography. Bodine was a youth hockey coach in the area.

### ***NEW TRENDS AND DEVELOPMENTS***

These scenarios are becoming more common. Predators are now using social networking sites and interactive gaming devices to prey upon young people. Websites such as MySpace.com, Facebook.com, and Xanga.com have recently become very popular with young people. Children use these sites to chat with friends, share photos, and post "blogs" - online journals about their interests, family and friends. Social networking figured prominently in the murder of Virginia Commonwealth University student Taylor Behl in 2005. It also facilitated the molestation of several girls in Middletown, Connecticut, in early 2006. The Computer Crime Section of the Virginia Attorney General's Office is currently working with law enforcement nationwide to educate parents and children on ways to safely use social networking sites.

In recent years, the interactive gaming industry has made major innovations in computer gaming. Players are no longer confined to competing solely against the computer or another person sitting in the room. New game systems like Xbox and PlayStation 3 allow users to participate in Internet gaming involving players from around the world, some of which use voice chat capabilities. As in Internet chat rooms, Internet gaming provides a certain degree of anonymity. Thus, predators can use this tool to contact potential victims.

Social networking and interactive gaming are two examples of new ways criminals misuse computers and the Internet to exploit children. Because of the Internet's prevalence in children's lives, the **Youth Internet Safety Task Force** seeks to safeguard it for them.

While child sexual exploitation may be the most insidious threat on the Internet, identity theft poses a serious risk and has become a relatively simple crime for enterprising criminals. As one of the fastest growing crimes in the United States, identity theft is perpetrated through database breaches, spam, peer-to-peer technology, and "phishing" schemes. Children's identities and personal identifying information such as Social Security numbers are particularly susceptible to such conduct. A new Federal Trade Commission report shows the number of victims under age 18 has doubled.<sup>6</sup> Virginia has responded by enacting laws to combat these threats and the **Youth Internet Safety Task Force** has worked to eliminate these crimes by encouraging the education of young people to limit the amount of personal identifying information they post online.

---

<sup>6</sup> Federal Trade Commission, *Identity Theft Victim Complaint Data: Figures and Trends* (2006).

Tracking computer criminals should not be the only responsibility of law enforcement. The vast technology sector has a vital role to play. Contemporaneous purging of e-mails and subscriber information for deleted online accounts is a too common practice of some Internet service providers. Some companies retain Internet Protocol connection logs for a fixed duration of time, but others do not retain the data at all. Such practices often hinder law enforcement investigations of many months. Longer retention of data is needed. It is the responsibility of business to assist in the apprehension of those who violate the promise of the Internet and prey upon children. Some Internet service providers and technology businesses have been eager to assist law enforcement. There is continuing need for ways of improving and streamlining procedures for disclosing pertinent information to create a more efficient process.

The Internet is the result of innovation; and innovation will also help businesses prevent criminal conduct. Social networking websites often have age requirements in order to use their services. Businesses must look to improve age verification procedures in order to better prevent underage children from gaining access to sites where they may post personal information and pictures of themselves. The most important party in protecting children is – as it has always been – parents. Parents are on the front lines in teaching leading, and protecting their children. This unique position must be used to promote Internet safety as well. The Task Force has found that Virginia parents, like parents nationwide, lack knowledge about the dangers of Internet predators and child pornographers. Many are also unaware of the numerous tools available to help prevent Internet predators from gaining easy access to their children. Often, parents do not realize that the websites their children visit, the information they post about themselves,

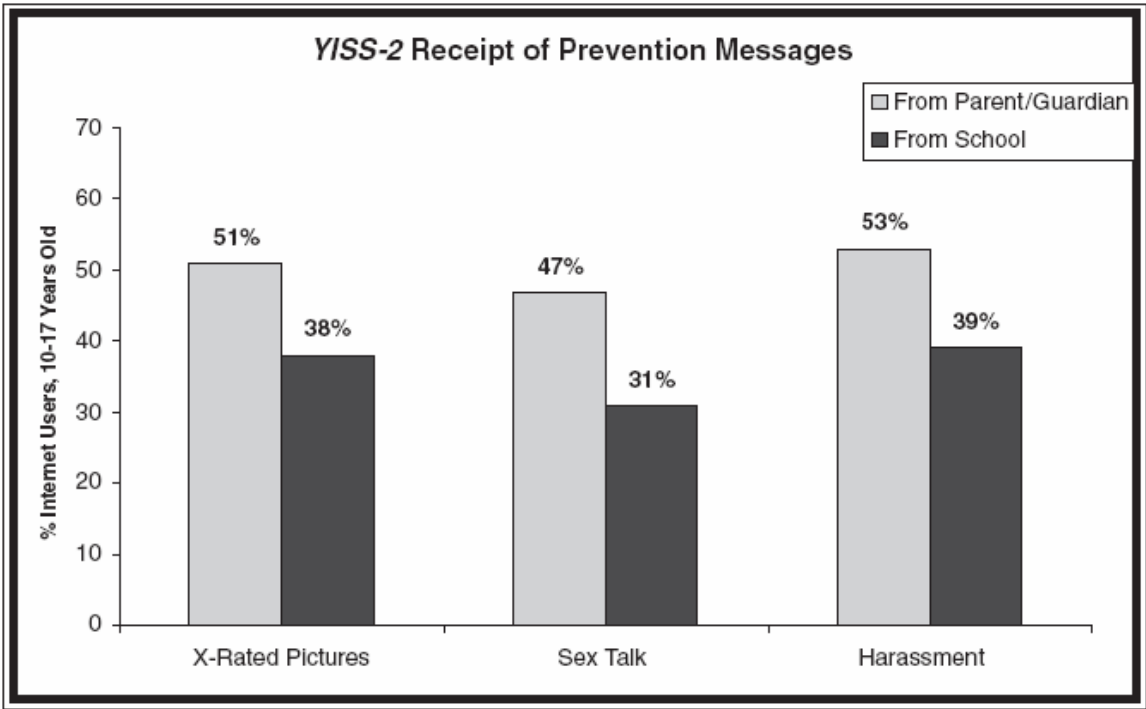
and their casual conversations with strangers can lead to danger. Furthermore, due to their perceived anonymity, many Virginia children fail to take seriously the imminent threat of sexual exploitation over the Internet.

In September 2006, the Virginia Department of Education took steps to increase awareness and understanding of Internet safety among children. In response to legislation passed by the 2006 Virginia General Assembly requiring local school divisions to teach Internet safety to students, the Department of Education developed guidelines for school divisions to follow when creating an Internet safety curriculum. These guidelines are contained in the booklet *Guidelines and Resources for Internet Safety in Schools*. While these guidelines are a significant step towards increasing awareness among children, it is only an initial step towards that goal. Supplemental action is needed to fully implement curricula that can effectively communicate the dangers facing children of all ages who attend public and private schools. Moreover, the guidelines are not designed to increase awareness among parents or to educate parents about the dangers of Internet predators. Additional initiatives are needed to increase parental awareness.

Child awareness of such dangers must be a multi-pronged approach and the message must originate from more than one source. A recent Youth Internet Safety Study (YISS-2) outlined the current state of awareness efforts. The study examined different types of dangers and where children were receiving prevention messages on each of the dangers. The following graph illustrates the findings<sup>7</sup>:

---

<sup>7</sup> J. Wolak, D. Finkelhor and K. Mitchell, *Online Victimization of Youth, Five Years Later*, p.60, (2005).



## **CURRENT VIRGINIA LAWS AND LAW ENFORCEMENT INITIATIVES**

The Virginia Code addresses two main areas of child exploitation: the sexual solicitation of children and child pornography. Virginia law prohibits the use of a communications system to solicit a minor in order to commit sexual conduct such as sodomy, commit indecent liberties if the child is less than 15 years of age, and manufacture, distribute, or possess child pornography. Law enforcement officers across Virginia routinely pose as children in Internet chat rooms to catch predators. The number of arrests is on the rise, as well as public awareness of the issue due to the Dateline news specials - "To Catch a Predator" - exposing these sexual predators. Virginia law fails to protect children ages 15-18 from most sexual solicitations. It also gives courts broad discretion when sentencing criminals, allowing a judge to suspend all of a sexual predator's prison time. This has led to inconsistent sentences across the Commonwealth. The **Youth Internet Safety Task Force** has confronted these problems with recommended legislation.

The Virginia Code also prohibits the possession, distribution, production, and reproduction of child pornography. Attorney General McDonnell's 2006 legislative package criminalized facilitating payment for online child pornography and made such a practice a felony. Virginia's laws attack the child pornography problem from both the supply and demand side. Yet, the child pornography laws fail to provide for mandatory minimum sentences for sexual predators. The variety of sentences handed

down around Virginia necessitates statutory revision. The Task Force has addressed this need.

Law enforcement agencies across the state assist in the identification of children in pornographic images. The National Center for Missing and Exploited Children based in Alexandria, Virginia, is instrumental in working with law enforcement on a worldwide level to identify and help the victims in these images. Unfortunately, the images of these child victims being sexually abused are permanent, graphic records that may exist in perpetuity on the Internet.

Identity theft is also prohibited in Virginia and, as noted earlier, poses another risk to children. Virginia law prohibits the unauthorized use of one's identifying information and makes such conduct a felony. In response to several major database breaches in 2005, the Attorney General proposed legislation which increased the penalties for identity theft when it involves multiple identities, a practice known as "pharming."

The fraudulent practices of sending Spam and "phishing" e-mails are also classified as felonies. The felony portion of the Spam statute prohibits falsification of e-mail routing information when combined with a statutory minimum amount of unsolicited e-mails sent in a designated timeframe. It also criminalizes as a felony sending obscene material through Spam and using a minor to send Spam. The "phishing" statute prohibits gathering identifying information using trickery or deception. E-mail crimes such as these pose a threat to children's financial futures.

Technologically savvy criminals actively seek to stay one step ahead of law enforcement. Virginia recognized the need to establish a specially trained and

equipped unit skilled in the investigation and prosecution of computer and Internet crimes. In 1999, the General Assembly established the Computer Crime Section within the Office of the Attorney General. The Section is comprised of prosecutors and investigators who handle computer crime and child exploitation cases across the Commonwealth. The Section's prosecutors are also cross-designated as Special Assistant United States Attorneys and routinely bring cases in federal court.

The Computer Crime Section is a founding partner and active participant in the Richmond-based Virginia Cyber Crime Strike Force which works closely with the United States Attorneys' Offices of the Eastern and Western Districts of Virginia along with the Federal Bureau of Investigation, United States Postal Inspection Service and Virginia State Police. The Strike Force investigates and prosecutes cases involving the online sexual solicitation of minors and child pornography in state and federal courts.

The Computer Crime Section has also become an important spokesman for computer crime and child exploitation awareness. Its members present an educational program titled "SafetyNet" on youth Internet safety and give talks on identity theft to schools, citizens, and law enforcement. In 2004, the Computer Crime Section received worldwide recognition after its members successfully prosecuted the nation's first felony Spam case in Loudoun County, Virginia. Its members serve on the National Association of Attorneys General executive committee addressing social networking. This group reviews social networking practices and encourages steps to make those sites safer for children.

## **MISSION**

The mission of the **Youth Internet Safety Task Force** has been to recommend methods to further protect the children and teenagers of Virginia through new laws and regulations, new tools and procedures for law enforcement, educational programs for schools, children and parents, and new business partnerships. To accomplish that mission, the Task Force has reviewed Virginia's existing child exploitation laws to ensure these laws adequately protect our youth and address the hazards of identity theft and threats to personal privacy.

The Task Force has developed new initiatives to educate parents and children on the dangers of the Internet. Additionally, the Task Force urges technology companies and Internet service providers in the "Digital Dominion" to devote resources and develop partnerships to advance youth Internet safety. By taking leadership in Virginia, the private sector can serve as a model for the rest of the country. It is vital that Virginia's business leaders, educators, government leaders, concerned citizens, parents, and law enforcement join together in the Attorney General's **Youth Internet Safety Task Force**. Virginia's children deserve no less.

## *Fast Facts About Youth and Internet Safety*

- 78.6% of Americans go online.<sup>1</sup>
- More than 20,000 images of child pornography are posted on the Internet each week.<sup>2</sup>
- The sexual exploitation of children on the Internet is a \$20 billion industry that continues to expand in the United States and abroad.<sup>3</sup>
- United States Attorney General Alberto Gonzales declared in May 2006, “There are as many as 50,000 predators online trolling for child sex victims at any given time.”
- One in five children, 10-17 years old, receive an unwanted sexual solicitation online.<sup>4</sup>
- One in thirty-three children, 10-17 years old, receive an aggressive sexual solicitation.<sup>5</sup>
- One in four 10-17 year olds had an unwanted exposure to pictures of naked people or people having sex.<sup>6</sup>
- Only 25% of youth who encountered a sexual solicitation tell a parent.

Of underage Internet users:

- 21% post e-mail addresses for all to see
- 11% post some personal information
- 8% purposely went to X-rated sites
- 7% sent pictures of themselves to someone they met online
- 5% posted pictures of themselves
- 4% talked about sex to a stranger<sup>7</sup>

---

<sup>1</sup> See Highlights of the 2005 Digital Future Report, USC Annenberg School Center for the Digital Future (2005), available at <http://www.digitalcenter.org/pdf/Center-for-the-Digital-Future-2005-Highlights.pdf>.

<sup>2</sup> United States Department of Justice, Project Safe Childhood, *Protecting Children from Online Exploitation and Abuse, part II, the Need for a National Initiative to Protect Children* (May 2006).

<sup>3</sup> Joshua Brockman, *Child Sex as Internet Fare, Through Eyes of a Victim*, *N.Y. Times*, (April 5, 2006).

<sup>4</sup> United States Department of Justice, *Highlights of the Youth Internet Safety Survey* (2006).

<sup>5</sup> J. Wolak, D. Finkelhor and K. Mitchell, *Online Victimization of Youth, Five Years Later* (2005).

<sup>6</sup> Crimes Against Children Research Center, *Online Victimization: A Report on the Nation's Youth* (June, 2000)

<sup>7</sup> *Id.*

- More than 80% of arrested child pornography possessors had images of prepubescent children.<sup>8</sup>
- 80% of arrested child pornography possessors had images of invasive sexual contact.<sup>9</sup>
- 21% of arrested child pornography possessors had images of bondage.<sup>10</sup>
- 39% of arrested child pornography possessors had videos.<sup>11</sup>
- 20% of images seized from child pornography possessors depict sexual exploitation of babies and 2-3 year-olds.<sup>12</sup>
- In a 2000 study in North Carolina, 71% of convicted child pornography offenders researched admitted molestation of significant numbers of children without detection.<sup>13</sup>
- The Sexually Exploited Child Unit of the L.A.P.D. conducted a 10-year study and found that adult and child pornography was used in 87% of child molestation cases.<sup>14</sup>
- Annual prosecutions of child pornography and child abuse cases rose more than 350% in the past decade.<sup>15</sup>
- Between 1996-2005 the number of child exploitation cases investigated by the FBI rose 2026%. There were similar jumps in arrests and an over 1000% jump in convictions.<sup>16</sup>
- President' Bush's fiscal year 2007 budget request seeks an increase of \$2.6 million for federal prosecution of exploitation and obscenity cases.

---

<sup>8</sup> J. Wolak, D. Rinkelhor & K. Mitchell, *Child Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study at 27* (2005).

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> J. Wolak, D. Rinkelhor, & K. Mitchell, *supra* note 10, at 4; see also [www.protectkids.com/dangers/stats.htm](http://www.protectkids.com/dangers/stats.htm).

<sup>13</sup> Andres E. Hernandez, Psy.D., *Self-Reported Contact Sexual Crimes of Federal Inmates Convicted of Child Pornography Offenses* (2000).

<sup>14</sup> See Long Island Citizens for Community Values, *Harms of Pornography*, [www.licco.org/pornisharmful.htm](http://www.licco.org/pornisharmful.htm) (Dec. 20, 2005).

<sup>15</sup> United States Department of Justice, Project Safe Childhood, *Protecting Children from Online Exploitation and Abuse, part II, the Need for a National Initiative to Protect Children* (May 2006).

<sup>16</sup> *Id.*

## HISTORY

In June 2006, Attorney General Bob McDonnell launched Virginia's Youth Internet Safety Task Force. The Task Force was comprised of distinguished technology, business, law enforcement, legislators, concerned parents and educators. The Attorney General directed the Task Force to convene town hall-style meetings in communities across the Commonwealth to hear about Internet safety from victims, citizens and interested parties about Internet safety.

The Task Force was charged with developing practical and effective ways to promote Internet safety and aid victims of Internet crimes. The Task Force was subdivided into three working groups: Law Enforcement, Technology, and Parent/Educator concerns. In keeping with the Attorney General's support of open government, all Task Force meeting minutes were posted on the Attorney General office's website and notices of meetings were posted on the Commonwealth Calendar. At each meeting there was an opportunity for the public to provide comments to the Task Force.

The Task Force convened five times from June through December 2006 in Northern Virginia, Hampton Roads, Roanoke and Central Virginia. Meetings included presentations by experts in particular subjects related to Internet safety, after which the Task Force divided into their working groups to make findings, recommendations and answer questions posed by the Attorney General, the public and other members of the Youth Internet Safety Task Force.

### **Law Enforcement Working Group**

The Law Enforcement Working Group focused on protecting children by strengthening Virginia's child exploitation laws and addressing concerns about inadequate law enforcement resources in child exploitation investigations. Specifically, the group recommended tougher punishment for sexual predators, recommended revising laws to criminalize certain conduct harmful to children, and explored ways to increase the number of computer forensic analysts and investigators who handle these crimes. The members of the Law Enforcement Working Group consisted of prosecutors, Internet service provider executives, public officials, and federal, state, and local law enforcement officers, all having experience with child exploitation crimes.

### **Parent/Education Working Group**

The Parent/Education Working Group consisted of public and private educators, law enforcement officials, concerned parents, students, Internet safety advocates, and religious leaders. The group focused on creating new and innovative ways to increase the awareness of both parents and children of the dangers posed by Internet predators and child pornographers. The group worked to provide parents with effective methods

and practical knowledge; enabling parents to protect their children when they travel the “information superhighway.”

### **Technology Working Group**

The breadth of experience in the Technology Working Group ranged from major international Internet service providers to social networking sites to government service and technological expertise. The Technology Working Group concentrated its work on identifying ways technology can assist law enforcement to track predators who use the internet to prey on children and developing methods to raise awareness of the parental controls and resources available to protect children online.

## *TASK FORCE WORKING GROUP ASSIGNMENTS*

### LAW ENFORCEMENT WORKING GROUP

The Law Enforcement Working Group focused on protecting children by strengthening Virginia's child exploitation laws and addressing concerns about inadequate law enforcement resources in child exploitation investigations. Specifically, the group toughened punishments for sexual predators, revised laws to criminalize certain conduct harmful to children and explored ways to increase the number of computer forensic analysts and investigators who handle these crimes. The members of the Law Enforcement Working Group consisted of prosecutors, Internet service provider executives, public officials, and federal, state and local law enforcement officers, all of whom have experience handling child exploitation crimes.

- **Honorable Robert Hurt, Member, House of Delegates, Martinsville, Pittsylvania and Henry Counties (Chair)**
- Honorable Mark D. Obenshain, Member, Senate of Virginia, Harrisonburg
- Chuck Rosenberg, U.S. Attorney, Eastern District of Virginia
- John L. Brownlee, U.S. Attorney, Western District of Virginia
- Honorable Mike Brown, Sheriff of Bedford County
- Honorable Eileen M. Addison, Commonwealth's Attorney for City of Yorktown
- Colonel W. Steve Flaherty, Superintendent of the Virginia State Police
- Colonel Rodney D. Monroe, Chief of the Richmond Police Department
- Robert E. Gwaltney, Assistant Special Agent in Charge, FBI
- John Ryan, Vice President and Associate General Counsel, America Online
- Michelle Collins, National Center for Missing and Exploited Children

## PARENTS/EDUCATORS WORKING GROUP

The Parent/Education Working Group consists of public and private educators, law enforcement officials, concerned parents, students, Internet safety advocates, and religious leaders. The group focused on creating new and innovative ways to increase the awareness of both parents and children of the dangers posed by Internet predators and child pornographers. In addition to creating an awareness of the dangers lurking on the Internet, the group worked to provide parents with effective methods and practical knowledge; enabling parents to protect their children when they travel the information superhighway.

- Stan Moorefield, Virginia Association of School Resource Officers
- Honorable Janet D. Howell, Member, Senate of Virginia, Fairfax
- Honorable Michael N. Herring, Commonwealth's Attorney City of Richmond
- Kenneth Booth, Concerned Parent
- Mary Alice Booth, Concerned Parent
- Rosemary Tribble, Community Leader
- William "Biff" Pusey, Concerned Parent
- Dr. Billy K. Cannaday, Jr., State Superintendent of Schools, Virginia Department of Education
- Dianne Florence, Virginia PTA President
- Dr. Sally K. Boese, Virginia Association of Independent Schools
- Mr. John Titus, Principal, James River High School
- James L. Hilton, Chief Information Officer, University of Virginia
- Virginia "Ginny" James, Cox High School, Government Teacher, Virginia Beach
- Donna Rice Hughes, President, Enough is Enough
- Dr. Steven Shelby, West End Presbyterian Church
- Carter Slough, Virginia High School Student
- Tommy Quigley, Virginia High School Student
- David Foster, Arlington School Board

## TECHNOLOGY PARTNER WORKING GROUP

The breadth of experience in the Technology Working Group ranges from major international internet service providers to social networking sites to government service and technological expertise. The Technology Working Group concentrated its work on identifying ways technology can assist law enforcement in deleting predators that use the internet to prey on children and methods to raise awareness of the parental controls and resources available to protect children online.

- **Robert J. Stolle, Executive Director, Greater Richmond Technology Council (Chair)**
- Honorable Ryan T. McDougle, Member, Senate of Virginia, Hanover County
- Honorable Kim Slayton-White, Commonwealth's Attorney Halifax County
- Charles D. Curran, Chief Counsel, Policy & Regulatory, America Online
- Anne Gavin, State Government Affairs Regional Manager, Microsoft Corporation
- Rick Lally, President, Hampton Roads Technology Council
- Elisabeth Bresee, Vice President and Senior Associate Counsel, Capital One
- Elizabeth Banker, Assistant General Counsel, Yahoo
- Bobbie Kilberg, President and CEO, Northern Virginia Technology Council
- Joel Wiginton, Vice President and Senior Associate for Government Affairs Sony
- Rick Lane, Vice President, Government Affairs, News Corporation-Myspace.com
- Ray LaMura, President, Virginia Cable Telecommunications Association
- Liz Eraker, Policy Analyst, Google Inc.

## SYNOPSIS OF TASK FORCE MEETINGS

### Alexandria, Virginia, July 2006

The Task Force met at the National Center for Missing & Exploited Children in Alexandria, Virginia on July 14, 2006, for its inaugural meeting. The National Center provided the facilities and amenities as its contribution to the Task Force's efforts.

Several speakers took to the podium first. The speakers were Ernie Allen, President, National Center for Missing & Exploited Children; John Ryan of AOL; Dr. Gary Reynolds, Operation Blue Ridge Thunder; and Donna Rice Hughes of Enough is Enough. Two concerned parents related the story of their child's involvement in Internet chat with a trusted teacher, who turned out to be an Internet predator subsequently sentenced to prison for the rest of his life.

Attorney General Bob McDonnell presented the mission of the Task Force, charging its members to contribute their personal and professional experience and expertise, with the goal of an agenda for improving Internet experiences for young people. *"Why is this important to Virginia? The estimates are anywhere from 40-50% of the world's Internet traffic goes through Northern Virginia. This is the information technology revolution epicenter. It is smart government for Virginia to do everything to protect the Internet to ensure that it stays the great agent of change and information, communication, electronic commerce, but not the safe haven of criminals. That is our challenge."* A period for public comment was allotted at which time several people in attendance made brief comments.

Two Virginia State Police special agents from the Northern Virginia Internet Crimes Against Children (ICAC) task force then gave a presentation which included one of the agents going live online into a chat room under the guise of a 14-year-old female. Within minutes, the pseudo-teen was engaged in a conversation with an allegedly 28-year-old male who immediately inquired if she had a webcam. Although she (the officer) repeatedly declined, the writer persisted in asking if he could send her his "picture." Ultimately, he sent his photo and an offer to see him on his webcam. Michelle Collins, Director of the Exploited Child Unit at NCMEC then gave a presentation containing disturbing data about the thousands of reports made to her organization weekly.

Lisa Hicks-Thomas of the Computer Crime Section of the Office of the Attorney General spoke about the role of her unit and its experiences in prosecuting child exploitation/child pornography cases throughout the Commonwealth. The Task Force then broke into the three pre-determined working groups: Law Enforcement; Technology Partners; and Parents and Educators.

## **Henrico, Virginia, September 2006**

The second meeting of the Task Force took place at Deep Run High School in Henrico County near Richmond. Delegate Bill Janis briefly welcomed the Task Force.

After Attorney General Robert F. McDonnell addressed the members of the Task Force, the Task Force heard three presentations. Sergeant Davenport of the Richmond Police Department. He spoke of his encounter with an Internet predator in the Richmond area and informed the Task Force about the general methods used by Internet predators to gain the trust of their victims.

Investigator Les Lauziere, with the Office of the Attorney General, Computer Crime Section, and Postal Inspector Glenn Aldridge, with the United States Postal Inspection Service, described the type of children predators target for exploitation.

Mr. John Ryan, Mr. Chris Bubb and Mrs. Jules Polonetsky of America Online explained the safeguards America Online has created to monitor Internet activity of persons who use their service. The presenters informed the Task Force that federal law mandates all Internet Service Providers to report child pornography activity to the National Center for Missing and Exploited Children.

Mrs. Betty Wade Coyle, with prevent Child Abuse Hampton Roads, addressed the Task Force as did a number of other citizens during the period set aside for public comment. Following the plenary session, the Task Force divided into working groups for further meetings.

While the Task Force conferred in another room, members of the Computer Crime Section presented the Office's SafetyNet program to several hundred high school students in the auditorium.

## **Virginia Beach, Virginia, October 2006**

The Task Force met at Cox High School in Virginia Beach for its third meeting.

Principal Dr. Brian K. Matney welcomed the Task Force to the school. Following this, Attorney General Bob McDonnell addressed the group.

During the public comment segment, Miss Virginia, Adrianna Sgarlata, spoke to the group about cyber-bullying and other youth Internet safety issues. She displayed a quilt with nine panels containing the names of Internet crime victims. Detectives Mike Encarnacao and Lisa Krisik of the Virginia Beach Police Department gave a presentation demonstrating the prevalence of sexual predators online. This was followed by a special presentation on the alarming increase of gang activity publicized and propounded through social networking websites.

The group broke into the three predetermined working groups. The Parents/Educators Working Group received a presentation by Donna Rice Hughes from Enough is Enough concerning “Rules & Tools” and some other safeguards available to schools and families. This working group then met jointly with the Technology Partners Working Group for a mid-task force comparison of findings and a joint question and answer period.

### **Roanoke, Virginia, November 2006**

The fourth meeting of the Task Force took place at Blue Ridge Television in the City of Roanoke. Attorney General McDonnell gave opening remarks and welcomed the group. Delegate William H. Fralin, Jr. spoke about his sponsorship of House Bill 58, which passed in the General Assembly and is now Virginia Code § 22.1-70.2. This law requires the Virginia Department of Education to create guidelines for teaching Internet safety in public schools throughout Virginia. Delegate Fralin commended the Virginia Department of Education and the Computer Crime Section of the Office of the Attorney General for creating these guidelines in an expedient manner and stated that its booklet was a model for the nation. The booklet was made available to all Task Force members.

Detective Mike Harmony of the Bedford County Sheriff’s Department gave a presentation about the successes of Operation Blue Ridge Thunder one of Virginia’s two ICACs (Internet Crimes Against Children Task Force). He illustrated the statistics of the operation and explained the challenges enforcing crimes against children.

The final presentation was given by Joe Showker, Instructional Technology Resource Teacher, with Rockingham County Public Schools. He provided the Task Force with a detailed presentation of the curriculum he uses to teach elementary and secondary public school students in Rockingham County about Internet safety. This curriculum includes using a video game educational tool provided by Web Wise Kids.

The main session ended and extended working group sessions followed.

### **Richmond, Virginia, September 2006**

The Youth Internet Safety Task Force met at the Office of the Attorney General for its final meeting. After calling the meeting to order, a member of each working group presented that group’s findings and recommendations to the entire body. After all three groups presented, the Task Force voted unanimously to adopt the entire package of recommendations, including legislative proposals. Attorney General McDonnell thanked the group for its work over the past six months and announced that an Advisory Committee would be created and its members named soon in order to implement the recommendations of the Task Force. The meeting was adjourned. The

next event will be the formal announcement and dissemination of the Report on December 20<sup>th</sup> at the Patrick Henry Building.

## *FINDINGS OF THE LAW ENFORCEMENT WORKING GROUP*

The Law Enforcement Working Group focused on protecting children by strengthening Virginia's child exploitation laws and addressing concerns about inadequate law enforcement resources in child exploitation investigations. Specifically, the group has recommended tougher punishments for sexual predators, recommended revising laws to criminalize certain conduct harmful to children and explored ways to increase the number of computer forensic analysts and investigators who handle these crimes. The members of the Law Enforcement Working Group were prosecutors, Internet service provider executives, public officials, and federal, state and local law enforcement officers, all of whom have experience handling child exploitation crimes.

## **Enact Mandatory Minimum Sentences for Sexual Predators**

The Law Enforcement Working Group heard evidence of the wide range of sentences for defendants in child pornography and online solicitation cases. The proliferation of child pornography and the ease with which sexual predators interact with children over the Internet are cause for concern. These disparities and the egregiousness of the offenses warrant statutory and mandatory minimum sentences. The group discussed the fiscal impact such measures would have on the Department of Corrections and obtained estimates from the Virginia Sentencing Commission based on the below proposals. The changes would have approximately a \$1.2 million impact over 10 years. During its deliberations, the working group also considered objections that mandatory sentences would ensnare teenagers in high school who engage in such conduct. Therefore, mandatory minimum sentences should apply to offenders who are at least 5 years older than the victim. Ultimately, the group recommended toughening laws prohibiting production and distribution of child pornography under Virginia Code §18.2-374.1 and online solicitation of children under Virginia Code §18.2-374.3.

### ***Recommendations:***

- 1. Amend Virginia Code §18.2-374.1 to include statutory and mandatory minimum sentences for production and financing of child pornography.**
- 2. Amend Virginia Code §18.2-374.3 to include statutory and mandatory minimum sentences for online solicitation of children. These mandatory minimums should be bifurcated for offenses involving child victims below 15 years of age and those involving children 15 to 18 years of age.**

### ***Virginia Code §18.2-374.1***

The age of the victim and the age of the offender in relation to the victim are the determining factors for mandatory minimum sentences. The specific language to be added as subsection (C) under §18.2-374.1 should be:

C. 1. Whoever violates this section, and the subject of the child pornography is a person less than 15 years of age, shall be punished by not less than 5 years nor more than 30 years in a state correctional facility. However, if the offender is at least 5 years older than the subject of the child pornography the offender shall be punished by a mandatory minimum term of imprisonment of not less than 15 years nor more than 30 years in a state correctional facility. Any offender who commits a second or subsequent violation of this subsection where the offender is at least 5 years older than the subject shall be punished by a mandatory minimum term of imprisonment of not less than 25 years nor more than 40 years.

2. Whoever violates this section, and the subject of the child pornography is a person at least 15 but less than 18 years of age, shall be punished by not less than 1 year nor more than 20 years in a state correctional facility. However, if the offender is at least 5 years older than the subject of the child pornography the offender shall be punished by a mandatory minimum term of imprisonment of not less than 5 years nor more than 30 years in a state correctional facility. Any offender who commits a second or subsequent violation of this subsection where the offender is at least 5 years older than the subject shall be punished by a mandatory minimum term of imprisonment of not less than 15 years nor more than 30 years.

*Virginia Code §18.2-374.1:1*

Distribution of child pornography, currently prohibited under §18.2-374.1(B)(4), should be moved to the possession of child pornography statute and contain mandatory minimum sentences. The language should read:

B. Any person who reproduces, sells, gives away, distributes, electronically transmits, displays with lascivious intent, purchases, or possesses with intent to sell, give away, distribute, transmit or display with lascivious intent child pornography shall be punished by not less than 5 years nor more than 20 years in a state correctional facility. Any person who commits a second or subsequent violation under this subsection shall be punished by a mandatory minimum term of not less than 5 years nor more than 20 years in a state correctional facility.

*Virginia Code §18.2-374.3*

The specific language to be added is:

[As part of a new subsection (B)] Whoever violates this subsection shall be guilty of a Class 5 felony. However, if the offender is at least 5 years older than the person he or she knows or has reason to believe is a child less than 15, the offender shall be punished by a mandatory minimum term of imprisonment of not less than 5 years nor more than 30 years in a state correctional facility. Any offender who commits a second or subsequent violation of this subsection where the offender is at least 5 years older than the person he or she knows or has reason to believe is a child less than 15 shall be punished by a mandatory minimum term of imprisonment of not less than 15 years nor more than 40 years.

C. It shall be unlawful for any person to use a communications system, including but not limited to computers or computer networks or bulletin boards, or any other electronic means, for the purposes of soliciting any person he or she knows or has reason to believe is a child at least 15 but less than 18 years of age for any of the activities listed in subsection B if the offender is at least 5 years older than the child. A violation of this subsection is a Class 5 felony. Any offender who commits a second or subsequent violation of this subsection shall be punished by a mandatory minimum term of imprisonment of not less than 1 nor more than 20 years.

D. It shall be unlawful for any person 18 years of age or older to use a communications system, including but not limited to computers or computer networks or bulletin boards, or any other electronic means, for the purposes of soliciting any person he knows or has reason to believe is a child less than 18 years of age for (i) any activity in violation of § 18.2-355 or § 18.2-361, (ii) activity in violation of § 18.2-374.1, or (iii) a violation of § 18.2-374.1:1.

Whoever violates this subsection shall be punished by a term of imprisonment of not less than 5 years nor more than 30 years in a state correctional facility. Any offender who commits a second or subsequent violation under this subsection shall be punished by a mandatory minimum term of imprisonment of not less than 5 years nor more than 30 years.

## Prohibit Online Solicitation of Children Ages 15-18

The Commonwealth's online solicitation statute, Virginia Code § 18.2-374.3, prohibits soliciting someone to engage in sexual conduct which would be a violation of §18.2-370, Taking Indecent Liberties with Children. Section 18.2-370 lists certain sexual conduct and prohibits engaging in such conduct with a child less than 15 years of age. Thus, online solicitation of children between the ages of 15 and 18 for certain sexual conduct is permitted in Virginia. The Law Enforcement Working Group heard evidence that, according to the National Center for Missing and Exploited Children, children ages 15-18 are the most solicited group by sexual predators over the Internet. The Virginia Code, in its current form, simply does not protect this age group. During its deliberations, the working group considered concerns that criminalizing such conduct with harsher mandatory penalties would ensnare some teenagers. Therefore, the harsher sentences should apply to offenders who are at least 5 years older than the victim.

### *Recommendation:*

**3. Amend Virginia Code §18.2-374.3 to prohibit sexual solicitations of children ages 15-18. The cross-reference to the indecent liberties statute should be eliminated and the language should be copied into §18.2-374.3. The age of the victim and the age of the offender in relation to the victim should be the determining factors for mandatory minimum sentences. The following language was approved by the working group as the new §18.2-374.3(B) and (C):**

B. It shall be unlawful for any person to use a communications system, including but not limited to computers or computer networks or bulletin boards, or any other electronic means, for the purposes of soliciting any person he or she knows or has reason to believe is a child less than 15 years of age in order to knowingly and intentionally:

(1) Expose his or her sexual or genital parts to any child to whom such person is not legally married or propose that any such child expose his or her sexual or genital parts to such person; or

(2) Propose that any such child feel or fondle the sexual or genital parts of such person or propose that such person feel or fondle the sexual or genital parts of any such child; or

(3) Propose to such child the performance of an act of sexual intercourse or any act constituting an offense under § 18.2-361; or

(4) Entice, allure, persuade, or invite any such child to enter any vehicle, room, house, or other place, for any of the purposes set forth in the preceding subdivisions of this section.

Whoever violates this subsection shall be guilty of a Class 5 felony. However, if the offender is at least 5 years older than the person he or she knows or has reason to believe is a child less than 15, the offender shall be punished by a mandatory minimum term of imprisonment of not less than 5 years nor more than 30 years in a state correctional facility. Any offender who commits a second or subsequent violation of this subsection where the offender is at least 5 years older than the person he or she knows or has reason to believe is a child less than 15 shall be punished by a mandatory minimum term of imprisonment of not less than 15 years nor more than 40 years.

C. It shall be unlawful for any person to use a communications system, including but not limited to computers or computer networks or bulletin boards, or any other electronic means, for the purposes of soliciting any person he or she knows or has reason to believe is a child at least 15 but less than 18 years of age for any of the activities listed in subsection B if the offender is at least 5 years older than the child. A violation of this subsection is a Class 5 felony. Any offender who commits a second or subsequent violation of this subsection shall be punished by a mandatory minimum term of imprisonment of not less than 1 nor more than 20 years.

## Prohibit Viewing Child Pornography Over the Internet

Virginia law is unclear as to whether viewing child pornography from the Internet without specifically downloading it onto one's computer is illegal. Thus, in some jurisdictions, child predators may continue to feed their habit of exploiting children, perpetuate the demand for child pornography over the Internet, and escape prosecution by simply viewing child pornography over the Internet. This conduct now includes a disturbing trend of people viewing live web-cam broadcasts of child sexual abuse over the Internet. The evidence of such conduct is normally found in a computer's temporary Internet cache. Change in the law is needed to ensure such conduct is prohibited.

### *Recommendation:*

#### **4. Amend Virginia Code §18.2-374.1(A) to include viewing child pornography over the Internet.**

The amended language should read:

“A.1. For the purposes of this article and Article 4 (§ 18.2-362 et seq.) of this chapter, the term "sexually explicit visual material" means a picture, photograph, drawing, sculpture, motion picture film, digital image, **including such material stored in a computer's temporary Internet cache or other volatile memory**, or similar visual representation which depicts sexual bestiality, a lewd exhibition of nudity, as nudity is defined in § 18.2-390, or sexual excitement, sexual conduct or sadomasochistic abuse, as also defined in § 18.2-390, or a book, magazine or pamphlet which contains such a visual representation. An undeveloped photograph or similar visual material may be sexually explicit material notwithstanding that processing or other acts may be required to make its sexually explicit content apparent.”

## Define “Child Pornography” and Consolidate Statutory Provisions

The consensus within the Law Enforcement Working Group is that sexually explicit visual material utilizing persons under 18 years of age should be described accurately: child pornography. Such a definition would both clarify and simplify the language contained in Article 5, Title 18.2 of the Virginia Code and would mirror the approach in the federal statutes.

After an in-depth review of the child exploitation statutes, the working group also recommends that certain sections be moved and consolidated for clarification and simplification.

### *Recommendation:*

**5. Amend Virginia Code §18.2-374.1 to include as subsection (A)(2) a separate definition of "child pornography" which would apply to the entire Article 5, Title 18.2 of the Virginia Code.**

The term “child pornography” would replace the phrase “sexually explicit visual material utilizing or having as a subject a person less than 18 years of age” wherever it is found in the Article. The amended language should provide:

2. For the purposes of this article, “child pornography” means sexually explicit visual material which utilizes or has as a subject a person less than 18 years of age.

Additionally, the distribution of child pornography under §18.2-374.1(B)(4) and reproduction of child pornography under §18.2-374.1(B)(3) should be moved to the possession of child pornography statute as the new §18.2-374.1:1(B). The facilitation for access to child pornography statute, §18.2-374.1:2, should also be included as the new §18.2-374.1:1(C). [See fully amended version at end of findings.]

## Allow Law Enforcement to Conduct Controlled Deliveries of Child Pornography

Virginia law currently prohibits law enforcement from conducting operations to apprehend those who have a propensity to possess child pornography. Such a practice is not prohibited under federal law and is frequently undertaken by federal agents. Controlled deliveries allow law enforcement officers who have reason to believe an individual is a child pornography collector, an opportunity to verify that the individual has a propensity to possess child pornography by giving him an opportunity to purchase child pornography through the mail. The practice is commonly used in drug cases by undercover local law enforcement officers.

### *Recommendation:*

**6. Amend Virginia Code §18.2-374.1:1 by striking the provision prohibiting prosecution after coming into possession of child pornography by a law enforcement officer. The language should read:**

**~~“A. Any person who knowingly possesses **child pornography** any sexually explicit visual material utilizing or having as a subject a person less than 18 years of age shall be guilty of a Class 6 felony. However, no prosecution for possession of material prohibited by this section shall lie where the prohibited material comes into the possession of the person charged from a law enforcement officer or law enforcement agency.”~~**

## Eliminate the Exceptions for "Permissible" Possession of Child Pornography

Child pornography, like drugs, is contraband. It is also a permanent record of a child's sexual abuse and each time the image is viewed the child is further exploited. The Law Enforcement Working Group agreed that there should be no specific classes of people (such as artists, sociologists, teachers, researchers, or students) who are permitted to possess child pornography. Federal law does not provide for such exceptions, nor do other sections of the code dealing with contraband. Those individuals who possess such material with the requisite criminal intent should be prosecuted.

### *Recommendation:*

#### **7. Amend Virginia Code §18.2-374.1:1 by striking subsection (B) which allows certain people to possess child pornography:**

~~B. The provisions of this section shall not apply to any such material which is possessed for a bona fide artistic, medical, scientific, educational, religious, governmental, judicial or other proper purpose by a physician, psychologist, sociologist, scientist, teacher, person pursuing bona fide studies or research, librarian, clergyman, attorney, judge, or other person having a proper interest in the material.~~

## Extend the Presumption of a Child's Age to the Possession of Child Pornography Statute

The Virginia statute prohibiting production, reproduction, and distribution of child pornography provides that a person who appears to be under 18 is presumed to be under 18. The Law Enforcement Working Group heard evidence that some prosecutors are hindered in *possession* of child pornography cases because this presumption is not extended to that statute. The group concluded that this presumption should logically be extended to the Virginia statute prohibiting possession of child pornography.

### *Recommendation:*

**8. Amend Virginia Code §18.2-374.1:1 by adding as subsection (E) the presumption language currently contained in §18.2-374.1. The provision would read:**

E. For the purposes of this section a person who is depicted as or presents the appearance of being less than eighteen years of age in sexually explicit visual material is prima facie presumed to be less than eighteen years of age.

## Expand Statutory Forfeiture of Equipment Used in Child Exploitation Crimes

Virginia Code §19.2-386.31 permits the seizure and forfeiture of equipment and other personal property used in connection with the production, distribution and sale of child pornography. However, forfeiture is not allowed in *possession* of child pornography cases or online solicitation cases.<sup>1</sup> The group recommends that the statute encompass forfeiture of tools used in these crimes.

### *Recommendation:*

9. Amend Virginia Code §19.2-386.31 to allow for forfeiture of equipment used in possession of child pornography and the online solicitation of children. The statute should also include a specific provision allowing a court to award such equipment to the seizing agency. The fully amended statute should read:

“§ 19.2-386.31. Seizure and forfeiture of property used in connection with **the exploitation and solicitation of** ~~production of sexually explicit items involving~~ children.

All audio and visual equipment, electronic equipment, devices and other personal property used in connection with the **possession**, production, distribution, publication, sale, possession with intent to distribute or making of **child pornography, as defined in § 18.2-374.1**, ~~sexually explicit visual material having a person less than 18 years of age as a subject~~ **or in connection with the solicitation of a person less than 18 years of age which constitutes a violation of § 18.2-374.3** shall be subject to lawful seizure by a law-enforcement officer and shall be subject to forfeiture to the Commonwealth pursuant to Chapter 22 (§ 19.2-369 et seq.) of this title by order of the court in which a conviction under § 18.2-374.1, **18.2-374.1:1 or 18.2-374.3** is obtained. Notwithstanding the provisions of § 19.2-381, the court shall dispose of the forfeited property as it deems proper, including awarding the property **to the agency seizing such property** or to a state agency for lawful purposes. If the property is disposed of by sale, the court shall provide that the proceeds be paid into the Literary Fund.

A forfeiture under this section shall not extinguish the rights of any person without knowledge of the illegal use of the property who (i) is the lawful owner or (ii) has a valid and perfected lien on the property.”

---

<sup>1</sup> Section 19.2-386.17 of the Code of Virginia already provides for the forfeiture of moneys, proceeds and income to third parties from computer crimes as well as computer equipment, software and all personal property used in connection with computer crimes. Additionally, Section 19.2-386.31 provides for the seizure and forfeiture of all equipment utilized in the production, distribution, publication, sale, and possession with intent to distribute child pornography.

## **Make Production of Child Pornography and Online Solicitation “Presumption of No Bond” Crimes**

Virginia Code §19.2-120 lists crimes where a judicial officer must presume that no bond should be granted to a defendant upon his arrest for one of those offenses. The defendant has the burden to produce evidence that he or she will not be a flight risk and will not be a danger to the community. The Law Enforcement Working Group agreed that production of child pornography, under the newly-amended version of § 18.2-374.1, and online solicitation crimes, under § 18.2-374.3, which are both crimes that will place a convicted defendant on the state’s sex offender registry, are sufficiently dangerous that violators of these statutes pose a great danger to children in the community.

### ***Recommendation:***

**10. Amend Virginia Code §19.2-120 to include production of child pornography and online solicitation as presumption of no bond crimes. The amended portions Virginia Code §19.2-120 should state:**

**8. A violation of § 18.2-374.1 or 18.2-374.3 where the child victim is under 15 years of age and the offender is at least 5 years older than the child victim;**

**8. 9. A violation of § 18.2-46.2, 18.2-46.3, 18.2-46.5 or 18.2-46.7; or**

**9. 10. A violation of § 18.2-36.1, 18.2-51.4, 18.2-266, or 46.2-341.24 and the person has, within the past five years of the instant offense, been convicted three times on different dates of a violation of any combination of these Code sections, or any ordinance of any county, city, or town or the laws of any other state or of the United States substantially similar thereto, and has been at liberty between each conviction.**

Approve the Fully Amended Version of § 18.2-374.1

*Recommendation:*

11. The Law Enforcement Working Group urges the approval of the fully amended version of the following statute, or a substantially similar version, with the aforementioned changes:

§ 18.2-374.1. Production, publication, sale, ~~possession with intent to distribute, financing, etc., of sexually explicit items involving children~~ **child pornography**; presumption as to age; severability.

A.1. For the purposes of this article and Article 4 (§ 18.2-362 et seq.) of this chapter, the term "sexually explicit visual material" means a picture, photograph, drawing, sculpture, motion picture film, digital image, **including such material stored in a computer's temporary Internet cache or other volatile memory**, or similar visual representation which depicts sexual bestiality, a lewd exhibition of nudity, as nudity is defined in § 18.2-390, or sexual excitement, sexual conduct or sadomasochistic abuse, as also defined in § 18.2-390, or a book, magazine or pamphlet which contains such a visual representation. An undeveloped photograph or similar visual material may be sexually explicit material notwithstanding that processing or other acts may be required to make its sexually explicit content apparent.

2. For the purposes of this article, "child pornography" means **sexually explicit visual material which utilizes or has as a subject a person less than 18 years of age.**

B. ~~A person shall be guilty of a Class 5 felony~~ **Any person** who:

1. Accosts, entices or solicits a person less than eighteen years of age with intent to induce or force such person to perform in or be a subject of **child pornography** ~~sexually explicit visual material~~; or

2. Produces or makes or attempts or prepares to produce or make **child pornography** ~~sexually explicit visual material which utilizes or has as a subject a person less than eighteen years of age~~; or

3. Who knowingly takes part in or participates in the filming, photographing or other reproduction of **child pornography** ~~sexually explicit visual material~~ by any means, including but not limited to computer-generated **child pornography** ~~reproduction, which utilizes or has as a subject a person less than eighteen years of age~~; or

4. ~~Sells, gives away, distributes, electronically transmits, displays with lascivious intent, purchases, or possesses with intent to sell, give away, distribute,~~

~~transmit or display with lascivious intent sexually explicit visual material which utilizes or has as a subject a person less than eighteen years of age~~

4. Knowingly finances or attempts or prepares to finance child pornography; shall be punished as provided in subsection C.

5. [Repealed.]

B1. [Repealed.]

~~C. A person shall be guilty of a Class 4 felony who knowingly finances or attempts or prepares to finance sexually explicit visual material which utilizes or has as a subject a person less than eighteen years of age.~~

**C. 1. Whoever violates this section, and the subject of the child pornography is a person less than 15 years of age, shall be punished by not less than 5 years nor more than 30 years in a state correctional facility. However, if the offender is at least 5 years older than the subject of the child pornography the offender shall be punished by a mandatory minimum term of imprisonment of not less than 15 years nor more than 30 years in a state correctional facility. Any offender who commits a second or subsequent violation of this subsection where the offender is at least 5 years older than the subject shall be punished by a mandatory minimum term of imprisonment of not less than 25 years nor more than 40 years.**

**2. Whoever violates this section, and the subject of the child pornography is a person at least 15 but less than 18 years of age, shall be punished by not less than 1 year nor more than 20 years in a state correctional facility. However, if the offender is at least 5 years older than the subject of the child pornography the offender shall be punished by a mandatory minimum term of imprisonment of not less than 5 years nor more than 30 years in a state correctional facility. Any offender who commits a second or subsequent violation of this subsection where the offender is at least 5 years older than the subject shall be punished by a mandatory minimum term of imprisonment of not less than 15 years nor more than 30 years.**

D. For the purposes of this section a person who is depicted as or presents the appearance of being less than eighteen years of age in sexually explicit visual material is prima facie presumed to be less than eighteen years of age.

E. The provisions of this section shall be severable and, if any of its provisions shall be held unconstitutional by a court of competent jurisdiction, then the decision of such court shall not affect or impair any of the remaining provisions.

Approve the Fully Amended Version of § 18.2-374.1:1

*Recommendation:*

**12. The Law Enforcement Working Group urges the approval of the fully amended version of the following statute, or a substantially similar version, with the aforementioned changes:**

§ 18.2-374.1:1. Possession, reproduction, distribution and facilitation of child pornography; penalty.

A. Any person who knowingly possesses **child pornography** ~~any sexually explicit visual material utilizing or having as a subject a person less than 18 years of age~~ shall be guilty of a Class 6 felony. **Any person who commits a second or subsequent violation under this subsection shall be guilty of a Class 5 felony.** ~~However, no prosecution for possession of material prohibited by this section shall lie where the prohibited material comes into the possession of the person charged from a law enforcement officer or law enforcement agency.~~

B. Any person who reproduces, sells, gives away, distributes, electronically transmits, displays with lascivious intent, purchases, or possesses with intent to sell, give away, distribute, transmit or display with lascivious intent child pornography shall be punished by not less than 5 years nor more than 20 years in a state correctional facility. Any person who commits a second or subsequent violation under this subsection shall be punished by a mandatory minimum term of not less than 5 years nor more than 20 years in a state correctional facility.

~~B. The provisions of this section shall not apply to any such material which is possessed for a bona fide artistic, medical, scientific, educational, religious, governmental, judicial or other proper purpose by a physician, psychologist, sociologist, scientist, teacher, person pursuing bona fide studies or research, librarian, clergyman, attorney, judge, or other person having a proper interest in the material.~~

C. Any person who intentionally operates an Internet website for the purpose of facilitating the payment for access to child pornography is guilty of a Class 4 felony.

D. All **child pornography** ~~sexually explicit visual material which utilizes or has as a subject a person less than 18 years of age~~ shall be subject to lawful seizure and forfeiture pursuant to § 19.2-386.31.

~~D. E. Any person convicted of a second or subsequent offense under this section shall be guilty of a Class 5 felony.~~ For the purposes of this section a person who is depicted as or presents the appearance of being less than eighteen years of age in sexually explicit visual material is prima facie presumed to be less than eighteen years of age.

~~§ 18.2-374.1:2. Facilitating payment for access to certain sexually explicit visual material; penalty.~~

~~Any person who intentionally operates an Internet website for the purpose of facilitating the payment for access to sexually explicit visual material that utilizes or has as a subject a person under the age of 18 years is guilty of a Class 4 felony.~~

**§ 18.2-374.1:2 [Repealed]**

**Approve the Fully Amended Version of § 18.2-374.3**

*Recommendation:*

**13. The Law Enforcement Working Group urges the approval of the fully amended version of the following statute, or a substantially similar version, with the aforementioned changes:**

§ 18.2-374.3. Use of communications systems to facilitate certain offenses involving children.

A. It shall be unlawful for any person to use a communications system, including but not limited to computers or computer networks or bulletin boards, or any other electronic means for the purposes of procuring or promoting the use of a minor for any activity in violation of § 18.2-370 or § 18.2-374.1. A violation of this subsection is a Class 6 felony.

~~B. It shall be unlawful for any person 18 years of age or older to use a communications system, including but not limited to computers or computer networks or bulletin boards, or any other electronic means, for the purposes of soliciting any person he knows or has reason to believe is a child less than 18 years of age for (i) any activity in violation of § 18.2-355 or § 18.2-361, (ii) any activity in violation of § 18.2-374.1, or (iii) a violation of § 18.2-374.1:1, or (iv) any activity in violation of subsection A of § 18.2-370.~~

**B. It shall be unlawful for any person to use a communications system, including but not limited to computers or computer networks or bulletin boards, or any other electronic means, for the purposes of soliciting any person he or she knows or has reason to believe is a child less than 15 years of age in order to knowingly and intentionally:**

**(1) Expose his or her sexual or genital parts to any child to whom such person is not legally married or propose that any such child expose his or her sexual or genital parts to such person; or**

**(2) Propose that any such child feel or fondle the sexual or genital parts of such person or propose that such person feel or fondle the sexual or genital parts of any such child; or**

**(3) Propose to such child the performance of an act of sexual intercourse or any act constituting an offense under § 18.2-361; or**

**(4) Entice, allure, persuade, or invite any such child to enter any vehicle, room, house, or other place, for any of the purposes set forth in the preceding subdivisions of this section.**

Whoever violates this subsection shall be guilty of a Class 5 felony. However, if the offender is at least 5 years older than the person he or she knows or has reason to believe is a child less than 15, the offender shall be punished by a mandatory minimum term of imprisonment of not less than 5 years nor more than 30 years in a state correctional facility. Any offender who commits a second or subsequent violation of this subsection where the offender is at least 5 years older than the person he or she knows or has reason to believe is a child less than 15 shall be punished by a mandatory minimum term of imprisonment of not less than 15 years nor more than 40 years.

C. It shall be unlawful for any person to use a communications system, including but not limited to computers or computer networks or bulletin boards, or any other electronic means, for the purposes of soliciting any person he or she knows or has reason to believe is a child at least 15 but less than 18 years of age for any of the activities listed in subsection B if the offender is at least 5 years older than the child. A violation of this subsection is a Class 5 felony. Any offender who commits a second or subsequent violation of this subsection shall be punished by a mandatory minimum term of imprisonment of not less than 1 nor more than 20 years.

D. It shall be unlawful for any person 18 years of age or older to use a communications system, including but not limited to computers or computer networks or bulletin boards, or any other electronic means, for the purposes of soliciting any person he knows or has reason to believe is a child less than 18 years of age for (i) any activity in violation of § 18.2-355 or § 18.2-361, (ii) any activity in violation of § 18.2-374.1, or (iii) a violation of § 18.2-374.1:1.

Whoever violates this subsection shall be punished by a term of imprisonment of not less than 5 years nor more than 30 years in a state correctional facility. Any offender who commits a second or subsequent violation under this subsection shall be punished by a mandatory minimum term of imprisonment of not less than 5 years nor more than 30 years.

As used in ~~this~~ subsections B, C and D, "use a communications system" means making personal contact or direct contact through any agent or agency, any print medium, the United States mail, any common carrier or communication common carrier, any electronic communications system, or any telecommunications, wire, computer, or radio communications system.

## Create a Regional Computer Forensic Lab in Richmond and Increase the Number of Forensic Analysts

Digital evidence continues to gain significance in a wide range of criminal investigations. This is attributable to the proliferation of high-technology and electronic devices such as computers, cell phones, personal digital assistants, digital cameras, and video recorders. Criminals are using these widely available and user-friendly devices to facilitate unlawful acts. As a result, investigators are encountering digital evidence in nearly every case, but it requires the special skills of a trained examiner to extract this evidence. Time-consuming extraction typically requires the use of forensic software programs and sophisticated electronic equipment. The key piece of evidence in child exploitation cases is typically the defendant's computer and, at times, the victim's computer. Most cases are built upon the results of forensic examinations of these computers.

Unfortunately, there is a shortage of trained computer forensic analysts in Virginia at the federal, state, and local levels of law enforcement. Computer forensic analysts have a backlog of computers and other digital evidence waiting to be examined. It can take several months between the time a defendant's computer is seized and the time a forensic examination of that computer is completed. Many times, a computer or other digital media can reveal evidence that the defendant is a danger to children, a fact that may not be known to law enforcement prior to the forensic examination. Additionally, the lag time can hinder prosecutors' attempts to have a defendant held without bond once probable cause to arrest the defendant is obtained from the computer evidence.

The Law Enforcement Working Group heard evidence of the above scenarios and recommends that a regional forensic lab housing local, state, and federal law enforcement officers should be created.

### *Recommendation:*

**14. Create a regional computer forensic lab to house local, state and federal law enforcement officers. The lab should contain examiners who are already trained in forensics and should include the addition of newly trained examiners. A regional lab will provide local law enforcement across Virginia a place to submit computers seized in *all* cases. Increasing the number of forensic analysts will help to reduce the backlog of cases that currently exists. The group further recommends that all the forensic analysts receive the same standard of certification. The level of certification should be reviewed for quality and approved by both prosecutors and law enforcement officers. Such a standard will help prevent attacks against the analysts' techniques in court.**

Funding of the lab is of paramount concern and several funding streams should be considered. The FBI currently has a Regional Computer Forensic Lab (RCFL) program where fourteen regional labs have been set up in twelve states around the country. These labs are federally funded and house local, state, and federal forensic examiners.<sup>2</sup> The closest FBI-funded Regional Computer Forensic Laboratory is located in Kentucky. Whether a Commonwealth of Virginia regional computer forensic laboratory is locally or federally controlled and housed are questions that should be answered during the regional forensic laboratory exploratory process. With a current budget surplus, there may be an opportunity to obtain state funds to start the lab. There exists potential for bi-partisan support for such a lab. Finally, funding from corporate partners should also be considered. Many technology based companies may be willing to contribute funds to such a worthy cause.

The working group recommends that the first lab should be located in Richmond, a central location in the state. The Virginia State Police has expressed a willingness to house the facility in Richmond and this possibility should be examined. The goal over the next several years should be to expand the concept to all regions of the state. Labs should be set up in Southwest Virginia, the Hampton Roads area and Northern Virginia.

---

<sup>2</sup> Such federal funding corresponds with a proposal contained in House Bill HR 4982 to establish an Office of Internet Safety and Public Awareness. The Office would, among other duties, provide technical assistance to local law enforcement in these cases.

## ***FINDINGS OF THE TECHNOLOGY PARTNERS WORKING GROUP***

The Technology Working Group's breadth of experience ranged from major international Internet Service Providers to Social Networking sites to government service and technological expertise. The Technology Working Group concentrated its work on identifying ways technology can assist law enforcement to track predators who use the Internet to prey on children and methods to raise awareness of the parental controls and resources available to protect children online.

### **Enable Law Enforcement to Intercept Wired Communications in cases involving the Sexual Exploitation of Minors**

The group's research reveals that while federal law allows states to intercept wired communication in most major felonies, such interception is only authorized for federal agencies in cases involving the sexual exploitation of minors. Before Virginia can amend its law, federal law must be amended to authorize states to intercept wired communication in cases involving sexual exploitation of minors.

#### ***Recommendations:***

1. ***Congress, and particularly Virginia's federal legislators should be encouraged to introduce legislation to amend Title 18 §2516(2) of the United States Code, enabling law enforcement to intercept wired communications in cases involving the sexual exploitation of minors.***
- (2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an ordering authorizing, or approving the interception of wire, oral or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, ***crimes that prohibit adults from communicating with children for the purpose of sexual exploitation, crimes that involve child pornography,*** or dealing with narcotic drugs, marijuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

*Recommendation:*

2. *After federal legislation is amended as described above, Virginia must amend §19.2-66 in accordance with the federal amendment to enable law enforcement to intercept wired communications in cases involving the sexual exploitation of minors.*

## Improving the Ability of Law Enforcement to Timely Obtain Information from Internet Service Providers

The Technology Working Group discussed the challenges faced by law enforcement in obtaining the technical evidence necessary to support prosecutions of child pornography cases. Virginia Internet Crimes Against Children Task Forces suggest maintaining Internet Protocol (IP) logs for a minimum of six months and ideally for one year due to the time required to serve legal documents on ISPs and communications service providers. The United States Internet Service Providers Association (USISPA) recommends reducing the required time for referrals to reach ISPs by enhancing the ability of investigative authorities to issue data preservation requests. The group also discussed some of the privacy concerns surrounding data retention, as well the potential cost implications of data retention to state government IT departments, public universities, and the private sector generally. One member of the Technology Working Group observed that they retain more data in one minute than many ISPs do in one year.

USISPA also pointed out that they are working on a federal proposal to allow the National Center for Missing and Exploited Children to send preservation of data requests directly to the ISPs. Some members noted this authority would clearly assist with cases referred through NCMEC but would not address cases reported directly to law enforcement.

### *Recommendation(s):*

3. *Providers of Internet access and communication services, both in the private and public sectors, should take measures to increase the likelihood of successful prosecution of Internet crimes involving child pornography and Internet predators by:*
  1. *Keeping data relevant to such investigations, and engaging at the national level to help define appropriate policies;*
  2. *Educating themselves about, and more extensively using, existing reporting channels for these crimes (particular the reporting requirements to the National Center for Missing and Exploited Children); and*
  3. *Improving the effectiveness of available data preservation mechanisms through increased awareness and training.*

## **Reduce the Time Required for Law Enforcement to Obtain Information from Electronic Communication Providers**

One of the alternatives to data retention discussed was that of authorizing other states to send search warrants directly to ISPs. Under current law, officers in other states must contact a Virginia law enforcement agency in order to obtain a search warrant for a Virginia ISP. Conversely, Virginia officers must locate officers in other states to execute search warrants on out-of-state ISPs. The end result is a bureaucratic challenge that increases time required for the search warrant to get to the ISP. The group reviewed the laws of four other states that have approved similar legislation.

### ***Recommendation:***

4. ***Enact Virginia Code § 19.2-56.2 to allow out-of-state search warrants to go directly to Internet Service Providers and allow Virginia search warrants to go directly to Internet Service Providers in other states.***

***§ 19.2-56.2. Warrant issued for search of provider of electronic communication service or remote computing services to the general public.***

- A. A business located in the Commonwealth that provides electronic communication services or remote computing services to the general public, when served with a warrant issued by another state to produce records that would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications, shall produce those records as if that warrant had been issued by a judge, magistrate or other person having the authority to issue such warrants in the Commonwealth.
- B. A warrant to may be issued in the Commonwealth for businesses located outside of the Commonwealth that provide electronic communication services or remote computing services to the general public for records that would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications.

## **Reduce the Time Required for Law Enforcement to Obtain Information from Electronic Communication Providers**

Another data retention alternative proposed was authorizing Virginia prosecutors and law enforcement officials to serve administrative subpoenas on Electronic Communication Providers. Under current law, officers must work with an attorney who will appear in court to obtain a court order from a circuit court seeking subscriber information. This increases the time necessary for public safety officials to obtain data. The group noted that federal prosecutors and federal law enforcement currently possess administrative subpoena authority to obtain subscriber information from Electronic Communication Providers.

### ***Recommendation:***

5. ***Enact Virginia Code § 19.2-10.2 to allow state prosecutors and law enforcement the ability to issue administrative subpoenas for subscriber information from Electronic Communication Providers***

§ 19.2-10.2. Administrative Subpoena issued for records from providers of electronic communication service or remote computing service.

- A. A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service, excluding the contents of electronic communications as required by § 19.2-70.3 , to a attorney for the Commonwealth or law-enforcement officer pursuant to an administrative subpoena issued pursuant to this section.
  1. In order to obtain such records, the attorney for the Commonwealth or law-enforcement official must certify there is reason to believe the records or other information sought are relevant to a legitimate law-enforcement inquiry.
  2. A court in the jurisdiction in the principal place of business of the electronic communication service or remote computing service, on a motion made promptly by the service provider, may quash or modify the order, if the information or records requested are unusually voluminous in nature or compliance with such order would otherwise cause an undue burden on such provider.
- B. No cause of action shall lie in any court against a electronic communication service or remote computing service., or enterprise, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a administrative subpoena under this section.

- C. Any and all records received by an attorney for the Commonwealth or law enforcement pursuant to this section shall be utilized only for a reasonable amount of time and only for a legitimate law-enforcement purpose. Upon the completion of the investigation the records held by the Commonwealth shall be destroyed if no prosecution is initiated.
- D. Nothing in this statute shall require disclosure of information in violation of federal law.

## **Reduce the Time Required for Law Enforcement to Obtain Information from Electronic Communication Providers**

One data retention alternative discussed was that of ensuring that prosecutors and law enforcement have the ability to obtain court orders for Electronic Communication Providers located outside of the Commonwealth. One of the speakers explained that some courts do not believe they have the authority under existing law to issue subpoenas for companies outside of the Commonwealth. The group researched this issue and noted that federal law authorizes any “court of competent jurisdiction” to issue orders for Electronic Communication Providers located in the United States.

### ***Recommendation:***

6. *Amend Virginia Code § 19.2-70.3(B) to allow courts to issue orders regarding subscriber information from Electronic Communication Providers located in or outside the Commonwealth*

- B. A court shall issue an order for disclosure under this section only if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant to a legitimate law-enforcement inquiry. *Any court of competent jurisdiction may issue orders for disclosure of records concerning electronic communication service or remote computing service providers located in or outside the Commonwealth.* A court issuing an order pursuant to this section , on a motion made promptly by the service provider, may quash or modify the order, if the information or records requested are unusually voluminous in nature or compliance with such order would otherwise cause an undue burden on such provider.

### ***Recommendation:***

7. *Amend Virginia Code § 19.2-70.3(A)(1) to give state prosecutors and law enforcement the ability to issue administrative subpoenas for subscriber information from Electronic Communication Providers*

1. A subpoena issued by an *attorney for the Commonwealth, law enforcement officer or grand jury* of a court of this Commonwealth;

## Eliminate the Ability of Convicted Sexual Offenders to Use e-mail Accounts Free of Public Scrutiny

The Technology Working Group discussed proscriptions that exist to keep sexual offenders away from minors. Current law does not prevent a convicted sex offender from assuming any identity online. Some companies review the sex offender registry in an attempt to keep predators away from minors. Myspace.com is currently seeking federal legislation that will *require* sex offenders to register their electronic mail addresses. Virginia does not require this registration. While this measure is not foolproof, members believed this would be another tool that could help Virginia keep predators away from children.

### *Recommendation:*

8. *Amend Virginia Code § 9.1-903 to require convicted sex offenders to register e-mail address, instant messaging identity, and other Internet communications identities, along with existing registration requirements*
- F. The registration shall be maintained in the Registry and shall include the person's name, all aliases that he has used or under which he may have been known, the date and locality of the conviction for which registration is required, his fingerprints and a photograph of a type and kind specified by the State Police, his date of birth, social security number, current physical and mailing address, *electronic mail address(es) and any instant messaging, chat or other Internet communication name(s) identities* and a description of the offense or offenses for which he was convicted. The registration shall also include the locality of the conviction and a description of the offense or offenses for previous convictions for the offenses set forth in § 9.1-902.

### *Recommendation:*

9. *Amend Virginia Code § 9.1-904 to require convicted sex offenders to reregister e-mail address, instant messaging identity, and other Internet communications identities, along with existing registration requirements*
- B. Any person convicted of a violation of § 18.2-472.1, other than a person convicted of a sexually violent offense or murder, shall reregister with the State Police every 180 days from the date of such conviction. Any person convicted of a violation of § 18.2-472.1, in which such person was included on the Registry for a conviction of a sexually violent offense or murder, shall reregister with the State Police every 30 days from the date of conviction. Re-registration means the person has notified the State Police, confirmed his current physical and mailing address *electronic mail address(es) and any instant messaging, chat or other Internet communication name(s) identities* and provided such other information, including identifying information, which the State Police may require. Upon registration and as may be necessary thereafter, the State Police shall provide the person with

an address verification form to be used for registration. The form shall state the registration requirements and contain in bold print a statement indicating that failure to comply with the registration requirements is punishable as provided in § 18.2-472.1.

## Increase Education with Safety Resources for Parents and Minors

The Technology Working Group discussed the measures they could take to protect children online. Most members currently take significant steps and provide comprehensive tools for parents and children. One member is about to launch a new operating system with parental controls to restrict all access by the computer. Another member offers parental controls that restrict all Internet access free of charge to anyone who wishes to download the controls. Not all customers are aware of these tools, make use of these tools, or know how to use them. The group noted that gaming and entertainment software is a burgeoning part of the Internet experience for young people after viewing a dynamic video game used for education of minors. The group felt that the implementation of video game would be an effective way to reach children.

### *Recommendations:*

10. *Develop a program that allows parents to receive Internet safety training. This Internet training should be made available on the Attorney General's website or another source that is readily available to the public. This training should also be available on television, in libraries and even in video stores. Virginia public and private schools should create positive incentives for maximum participation.*
11. *Partnerships should be sought with Virginia public and private schools for training and distribution with dynamic Internet safety video games.*
12. *Recommend that the General Assembly issue a resolution announcing October as Internet Safety Awareness Month. Parents should review filters and ensure parental controls are installed and updated during this month.*

## **Reduce the Ability of Adults to Communicate with Minors Online**

One of the most challenging issues facing the Technology Working Group was that of age verification. It is very difficult to verify the age of users under 18 due to the lack of any public databases against which to match their online registration information. The group discussed some of the procedures currently used to monitor Internet use, such as parental controls, filters and credit cards, although none of these approaches is specifically designed to verify a user's age. The group discussed implementing credit card verification of account holders as the standard for age verification. Some companies require credit card verification before a customer can chat online with other customers. Nonetheless, this assumes the person who uses the credit card is the cardholder and not all customers own credit cards. The group discussed implementing a government-issued number such as passport number, driver's license number, etc. to identify the age of customer. Given that most of the companies have global customers, this option is not practical as well as created potential privacy concerns. In addition, it would remain unknown if the account holder was the true holder of the number. The group ended the discussion noting that there is no perfect solution to this problem, but all recognize the need for some type of age verification.

### ***Recommendation:***

- 13. Electronic Communication Providers should continue to pursue technology to identify and verify the age of customers***

## FINDINGS OF THE PARENT/EDUCATION WORKING GROUP

The Parent/Education Working Group consists of public and private educators, law enforcement officials, concerned parents, students, Internet safety advocates, and religious leaders. The group focused on creating new and innovative ways to increase the awareness of both parents and children of the dangers posed by Internet predators and child pornographers. In addition to creating an awareness of the dangers lurking on the Internet, the group worked to provide parents with effective methods and practical knowledge; enabling parents to protect their children when they travel the information superhighway.

### Ensure the Internet Safety Curriculum Adopted by Local School Divisions Adequately Educates Students about the Dangers Posed by the Internet and Establish a Method by which Local School Divisions and Private Schools have Access to Internet Safety Curricula Developed and Utilized by Other School Divisions in Virginia

Delegate William Fralin apprised the Task Force of legislation he sponsored, House Bill 58, which was passed by the 2006 Virginia General Assembly and made a part of Code § 22.1-70.2. House Bill 58 requires local school divisions to instruct students on Internet Safety consistent with the guidelines issued by the Superintendent of Public Instruction. Working group member Dr. Billy K. Cannaday, Jr, State Superintendent of Schools, advised the working group that the Virginia Department of Education developed guidelines for school divisions regarding instructional programs related to Internet safety in response to the new legislation. These guidelines are contained in a booklet titled *Guidelines and Resources for Internet Safety in Schools*, which was developed by the Virginia Department of Education with assistance from many partners, including the Office of the Attorney General. Local school divisions must create Internet safety curriculum within these guidelines. It is imperative that any Internet safety curriculum adopted by local school divisions effectively communicate the dangers facing children to students, K through 12, attending public and private schools throughout Virginia. Furthermore, public and private schools should have access to successful curricula developed by counterpart school divisions.

#### *Recommendation:*

- 1. The Attorney General should work with the Virginia Department of Education to assist local school divisions in developing their own methods for teaching Internet Safety to elementary and secondary students, as well as parents, which are within the guidelines established by the Virginia Department of Education.**

*Recommendation:*

2. **The Attorney General should work with the Virginia Department of Education to establish best practices for teaching Internet safety and make those best practices and other resources, including sample curricula on Internet safety, available to public and private schools throughout Virginia**

**Sponsor a Contest for Children Attending Public and Private Schools in Virginia to Produce Multimedia Materials to Increase Awareness of Internet Safety among Children and Parents and to Provide Practical Safety Solutions to Parents and Children**

An important objective of Internet safety awareness programming and education is to convey to students information about dangers they face while using the Internet in such a manner as to encourage them to change the way they use the Internet. The working group learned that all too often the numerous messages communicated to students regarding Internet safety fail to change how students use the Internet. Students continue to have the “it won’t happen to me” attitude toward Internet dangers. The two teenage student task force members in the working group confirmed this conclusion. The best way to communicate Internet dangers to elementary and secondary students in order to pierce this rationalization, the working group concluded, is to give students a prominent role in the creation of the message. Additionally, the working group concluded that an Internet safety message created by students would be another method to inform parents about Internet safety.

***Recommendation:***

- 3. The Attorney General should work with the Virginia Department of Education, the Virginia Association of Independent Schools, and others to sponsor a statewide contest among elementary and secondary students attending public and private schools, as well as home-schooled students, to produce multimedia materials, including but not limited to public service announcements and videos, targeted at students and parents to increase awareness of Internet dangers and provide practical safety solutions to parents and children.**

## Existing Venues to Inform and Educate Parents Regarding Internet Safety

The working group determined that despite the safety information available on the Internet, too many Virginia parents are insufficiently informed of the dangers Internet predators pose to children. These parents lack adequate knowledge of the tools available to protect children from Internet predators. In order to better communicate this vital information to parents, the working group identified four existing venues to reach parents with information to increase awareness of the dangers children face on the Internet and notify them of safety tools available. These categories are Private Employers, Health and Welfare Organizations, Religious Organizations, and State Agencies.

One method for reaching large Virginia companies and state agencies is to train members of their respective human resource departments on Internet safety related to children. The companies and agencies could hold forums in which the trained human resource employee would educate other employees on Internet Safety. Similarly, small Virginia businesses could be identified and contacted through regional chambers of commerce throughout Virginia. Education materials and training would be provided to regional chambers of commerce which would, in turn, distribute those materials to their members.

An informational leaflet or an educational compact disk can be provided to health and welfare organizations, religious organizations, and state agencies throughout Virginia. Those organizations would then circulate and distribute the informational leaflets and educational compact disks. The leaflet and compact disk would contain some useful tips on protecting children who use the Internet, as well as a toll free number and a website where the reader could obtain more detailed information.

### *Recommendation:*

- 4. The Attorney General should establish partnerships with Virginia private employers, health and welfare organizations, faith based organizations, and Virginia state agencies to increase awareness among parents of the dangers children face on the Internet and educate parents about safety rules and tools parents can utilize to protect children from these dangers.**

## **Targeted Statewide Media Campaign**

The general public in Virginia is not sufficiently aware of the serious dangers Internet predators pose to children who use the Internet. A targeted statewide media campaign is essential to increasing awareness among parents and children so that those groups are receptive to the specific informational and educational initiatives proposed by this working group.

### *Recommendation:*

- 5. The Attorney General should lead a statewide media campaign funded by public/private partnerships targeting parents and children to increase awareness among parents and children of the dangers posed by online predators, child pornography and other obscene materials. The media campaign should include but not be limited to radio ads, billboard ads, public transit ads, full page ads in major Virginia newspapers, and public service announcements for cable and broadcast television and Internet ads.**

It is imperative that the recommendations made by the Parent/Education Working Group be fully implemented. To ensure timely and effective implementation of each of these recommendations, the working group recommends that the Attorney General establish an implementation/advisory team tasked with developing and supervising the execution of the Internet Safety awareness and education campaign.

### *Recommendation:*

- 6. The Attorney General should, without delay, establish an implementation/advisory team consisting of public and private educators, concerned parents, students, Internet safety advocates, members of the faith-based community, state legislators, leaders in the technology industry, and law enforcement officials to develop and supervise the execution of each recommendation from the Parent/Education Working Group.**

## RECOMMENDATIONS

### *Law Enforcement Working Group*

1. *Amend Virginia Code §18.2-374.1 to include statutory and mandatory minimum sentences for production and financing of child pornography.*
2. *Amend Virginia Code §18.2-374.3 to include statutory and mandatory minimum sentences for online solicitation of children. These mandatory minimums should be bifurcated for offenses involving child victims below 15 years of age and those involving children 15 to 18 years of age.*
3. *Amend Virginia Code §18.2-374.3 to prohibit sexual solicitations of children ages 15-18. The age of the victim and the age of the offender in relation to the victim should be the determining factors for mandatory minimum sentences.*
4. *Amend Virginia Code §18.2-374.1(A) to include viewing child pornography over the Internet.*
5. *Amend Virginia Code §18.2-374.1 to include as subsection (A)(2) a separate definition of "child pornography" which would apply to the entire Article 5, Title 18.2 of the Virginia Code.*
6. *Amend Virginia Code §18.2-374.1:1 by striking the provision prohibiting prosecution after coming into possession of child pornography by a law enforcement officer permitting controlled deliveries to child pornography collectors.*
7. *Amend Virginia Code §18.2-374.1:1 by striking subsection (B) which allows certain people to possess child pornography*
8. *Amend Virginia Code §18.2-374.1:1 (possession of child pornography) by adding as subsection (E) the presumption that a child appearing under 18, is under 18, currently contained in §18.2-374. (production and reproduction of child pornography)1.*
9. *Amend Virginia Code §19.2-386.31 to allow for forfeiture of equipment used in possession of child pornography and the online solicitation of children. The statute should also include a specific provision allowing a court to award such equipment to the seizing agency.*
10. *Amend Virginia Code §19.2-120 to include production of child pornography and online solicitation as presumption of no bond crimes.*

11. *Create a regional computer forensic lab to house local, state and federal law enforcement officers. The lab should contain examiners who are already trained in forensics and should include the addition of newly trained examiners. A regional lab will provide local law enforcement across Virginia a place to submit computers seized in all cases.*

## Technology Working Group

1. *Congress, and particularly Virginia's federal legislators should be encouraged to introduce legislation to amend Title 18 §2516(2) of the United States Code, enabling law enforcement to intercept wired communications in cases involving the sexual exploitation of minors.*
2. *After federal legislation is amended as described above, Virginia must amend §19.2-66 in accordance with the federal amendment to enable law enforcement to intercept wired communications in cases involving the sexual exploitation of minors.*
3. *Providers of Internet access and communication services, both in the private and public sectors, should take measures to increase the likelihood of successful prosecution of Internet crimes involving child pornography and Internet predators*
4. *Enact Virginia Code § 19.2-56.2 to allow out-of-state search warrants to go directly to Internet Service Providers and allow Virginia search warrants to go directly to Internet Service Providers in other states.*
5. *Enact Virginia Code § 19.2-10.2 to allow state prosecutors and law enforcement the ability to issue administrative subpoenas for subscriber information from Electronic Communication Providers*
6. *Amend Virginia Code § 19.2-70.3(B) to allow courts to issue orders regarding subscriber information from Electronic Communication Providers located in or outside the Commonwealth*
7. *Amend Virginia Code § 19.2-70.3(A)(1) to give state prosecutors and law enforcement the ability to issue administrative subpoenas for subscriber information from Electronic Communication Providers*
8. *Amend Virginia Code § 9.1-903 to require convicted sex offenders to register e-mail address, instant messaging identity, and other Internet communications identities, along with existing registration requirements*
9. *Amend Virginia Code § 9.1-904 to require convicted sex offenders to reregister e-mail address, instant messaging identity, and other Internet communications identities, along with existing registration requirements*
10. *Develop a program that allows parents to receive Internet safety training. This Internet training should be made available on the Attorney General's website or another source that is readily available to the public.*

11. *Partnerships should be sought with Virginia public and private schools for training and distribution with dynamic Internet safety video games.*
12. *Recommend that the General Assembly issue a resolution announcing October as Internet Safety Awareness Month.*
13. *Electronic Communication Providers should continue to pursue technology to identify and verify the age of customers.*

## Parent/Education Working Group

1. *The Attorney General should work with the Virginia Department of Education to assist local school divisions in developing their own methods for teaching Internet Safety to elementary and secondary students, as well as parents, which are within the guidelines established by the Virginia Department of Education.*
2. *The Attorney General should work with the Virginia Department of Education to establish best practices for teaching Internet safety and make those best practices and other resources, including sample curricula on Internet safety, available to public and private schools throughout Virginia*
3. *The Attorney General should work with the Virginia Department of Education, the Virginia Association of Independent Schools, and others to sponsor a statewide contest among elementary and secondary students attending public and private schools, as well as home-schooled students, to produce multimedia materials, including but not limited to public service announcements and videos, targeted at students and parents to increase awareness of Internet dangers and provide practical safety solutions to parents and children.*
4. *The Attorney General should establish partnerships with Virginia private employers, health and welfare organizations, faith based organizations, and Virginia state agencies to increase awareness among parents of the dangers children face on the Internet and educate parents about safety rules and tools parents can utilize to protect children from these dangers.*
5. *The Attorney General should lead a statewide media campaign funded by public/private partnerships targeting parents and children to increase awareness among parents and children of the dangers posed by online predators, child pornography and other obscene materials. The media campaign should include but not be limited to radio ads, billboard ads, public transit ads, full page ads in major Virginia newspapers, and public service announcements for cable and broadcast television and Internet ads.*
6. *The Attorney General should, without delay, establish an implementation/advisory team consisting of public and private educators, concerned parents, students, Internet safety advocates, members of the faith-based community, state legislators, leaders in the technology industry, and law enforcement officials to develop and supervise the execution of each recommendation from the Parent/Education Working Group.*

## CONCLUSION

As the Youth Internet Safety Task Force has learned, Internet dangers affect Virginians and, particularly, children and teenagers across the Commonwealth with disturbing frequency and sometimes devastating results. Internet crimes are increasing exponentially and part of law enforcement's greatest challenge is keeping up with the cyber criminals. This Report's recommendations and findings made by an erudite and broad cross-section from Virginia are a first step toward addressing Youth Internet safety.

Much work remains to be done. The Advisory Committee recommended by the parents and educators who served on this Task Force will carry the torch in the months and years to follow. A statewide multimedia campaign, which is asymmetrical in its approach and wide in its reach, will educate parents, students and the general population of Virginia and beyond on many important subjects and dangers related to the Internet. The proposal of mandatory minimum sentences for certain child exploitation crimes and the registration of sex offenders' e-mail addresses in addition to more helpful legislation for Internet Service Providers to accommodate administrative subpoenas are just some of the recommendations that will help ensure that youth in Virginia and across the country are better protected from Internet criminals and child predators.

As we move ahead, Attorney General McDonnell and the Advisory Committee are committed to making these strides and others to "fight the good fight" with respect to Internet safety and to better protect Virginia children. Attorney General McDonnell thanks each of the citizens who served on the Task Force for their wise and valuable counsel in this endeavor.

# APPENDIX

## \*A\*



## LINKS AND RESOURCES FOR PARENTS AND EDUCATORS (Reprinted with permission of the Virginia Department of Education)

### Web-Based Resources on Internet Safety

This appendix lists Web sites related to Internet safety. All Web sites were accurate and online as of 13 August 2006.

#### Age-Appropriate Guidelines for Internet Use

*Be Web Aware* by Media Awareness Network (see Safety Tips by Age on left side of screen)

<http://www.bewebaware.ca/english/default.aspx>

- Safety tips by age (left-side menu)

*GetNetWise: Online Safety Guide* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/>

- A parent's perspective and information about online privacy

*A Parent's Guide to Online Safety: Ages and Stages* by Microsoft

<http://www.microsoft.com/athome/security/children/parentsguide.msp>

- Guide to how children of different ages use the Internet

#### Copyright (see Ethics)

#### Cyberbullying

*Be Web Aware: Challenging Cyber Bullying* by Media Awareness Network

<http://www.bewebaware.ca/english/CyberBullying.aspx>

- Legal overview, role of Internet service providers, and taking action

*Cyberbullies* by National Crime Prevention Council

<http://www.mcgruff.org/ProblemSolver/cyberbully.htm>

- Tips for avoiding and handling cyberbullies

Cyberbullying handouts [untitled] by Bullying.org

[http://www.cyberbullying.org/pdf/Cyberbullying\\_Information.pdf](http://www.cyberbullying.org/pdf/Cyberbullying_Information.pdf)

- Details about cyberbullying (Canadian)

*OnGuard Online—US CERT Tip: Dealing with Cyberbullies* by United States Computer Emergency Readiness Team

<http://www.onguardonline.gov/certtips/st06-005.html>

- Recognition of and protection from cyberbullies

*STOP cyberbullying* by WiredKids

<http://www.stopcyberbullying.org/index2.html>

- Legal overview, prevention, and reporting

#### Definitions

*BeWebAware: Internet 101* by Media Awareness Network

<http://www.bewebaware.ca/english/internet101.aspx>

- Short glossary of several Internet terms

*Glossary* by Symantec

<http://securityresponse.symantec.com/avcenter/refa.html>

- Extensive glossary of computer terms

*Internet Definitions* by Netsmartz

<http://www.netsmartz.org/safety/definitions.htm>

- Extensive online glossary

*The Librarian's Guide to Great Web Sites for Kids* by American Library Association

<http://www.ala.org/parentspage/greatsites/guide.html>

- Definitions of new technologies (end of paper)

*OnGuard Online: Glossary* by Federal Trade Commission

<http://onguardonline.gov/glossary.html>

- Standard glossary of computer terms

#### E-mail

*BeWebAware: Spam* by Media Awareness Network

<http://www.bewebaware.ca/english/spam.aspx>

- Tips for parents regarding *spam*

*GetNetWise: Risks by Technology: Email* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/technology/email>

- Basic overview of *spam* and junk mail

*Help keep spam out of your inbox* by Microsoft

<http://www.microsoft.com/athome/security/email/fightspam.aspx>

- Tips and filters for blocking junk mail

*OnGuard Online: Spam Scams* by Federal Trade Commission

<http://onguardonline.gov/spam.html>

- List of popular scams and recommendations for avoiding problems

*Sorted: Keep your information secure online* by Childnet International

<http://www.childnet-int.org/sorted/>

- Maintaining student safety and privacy

### **Ethics**

*Cyberethics* by U.S. Department of Justice, Computer Crime & Intellectual Property Section

<http://www.cybercrime.gov/cyberethics.htm>

- Links to sites about *cybercrime*

*RespectCopyrights.org* by Motion Picture Association of America

<http://www.respectcopyrights.org/content.html>

- Issues involved with illegal downloads

### **Filtering**

*BeWebAware: Get the Most out of the Internet: Technological Tools* by Media Awareness Network

[http://www.mediaawareness.ca/english/teachers/wa\\_teachers/safe\\_passage\\_teachers/getmost\\_techtools.cfm](http://www.mediaawareness.ca/english/teachers/wa_teachers/safe_passage_teachers/getmost_techtools.cfm)

- Checklist for evaluating content-management products and related issues

*Filtering and Blocking* by WiredKids

<http://www.wiredkids.org/safesites/filtering.html>

- Information about filtering, blocking, and outgoing software

*FilterReview.com* by National Coalition for the Protection of Children and Families

<http://www.filterreview.com/index.htm>

- Background for selecting the most appropriate filters

“Why Filters Won’t Protect Children or Adults” by Nancy Kranich, *Library Administration and Management* 18(1): 14-18 (published by American Library Association)

<http://www.ala.org/ala/oif/ifissues/issuesrelatedlinks/whyfilterswontprotect.htm>

- Educating about Internet safety as opposed to using filters

### **Hate Sites**

*BeWebAware: Violent and Hateful Content* by Media Awareness Network

<http://www.bewebaware.ca/english/violent.aspx>

- Information about violent content, online hate, and what parents should do

*WHOIS Search* by Network Solutions

<http://www.networksolutions.com/whois/index.jsp>

- Search engine to determine ownership of domain names

### **Identity Theft**

*Help prevent identity theft from phishing scams* by Microsoft

<http://www.microsoft.com/athome/security/email/phishingemail.aspx>

- Basic overview of *phishing* scams

*Keep Your Identity To Yourself* by National Crime Prevention Council

[http://www.ncpc.org/media/Identity\\_Theft.php](http://www.ncpc.org/media/Identity_Theft.php)

- Free download of *Preventing Identity Theft: A Guide for Consumers*

*OnGuard Online: ID Theft* by Federal Trade Commission

<http://onguardonline.gov/idtheft.html>

- Steps to take in case of identity theft

*Your National Resource about Identity Theft* by Federal Trade Commission

<http://www.consumer.gov/idtheft/>

- Resources about identity theft, including printable brochure and PowerPoint slides

### **Instant Messaging**

*10 tips for safer instant messaging* by Microsoft

<http://www.microsoft.com/athome/security/online/imsafety.aspx>

- Suggestions for using instant messaging

## **International, National, and State Organizations**

*ChildNet International Home Page*

<http://www.childnet-int.org>

*Cyberbullying.org*

<http://www.cyberbullying.org/>

*Cybercitizenship.org*

<http://www.cybercitizenship.org/index.html>

*Cyberethics, Cybersafety, Cybersecurity (C3) Institute* by University of Maryland, College of Education

<http://www.edtechoutreach.umd.edu/C3Institute/c3resources.html>

*Family Internet Safety* by Attorney General of Virginia

[http://www.oag.state.va.us/KEY\\_ISSUES/FAMILY\\_INTERNET/index.html](http://www.oag.state.va.us/KEY_ISSUES/FAMILY_INTERNET/index.html)

*GetNetWise* by Internet Education Foundation

<http://www.getnetwise.com/>

*Internet Safety* by Polly Klaas Foundation

<http://www.pollyklaas.org/internet-safety/index.html>

*i-SAFE* by Internet Safety Foundation

<http://www.isafe.org/>

*Justice for Kids & Youth* by U.S. Department of Justice

<http://www.usdoj.gov/kidspage/>

*Kidz Privacy* by Federal Trade Commission

<http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html>

*National Center for Missing & Exploited Kids Home Page*

<http://www.missingkids.com/>

*NetSmartz* by National Center for Missing & Exploited Kids

<http://www.netsmartz.org/>

*OnGuard Online* by Federal Trade Commission

<http://onguardonline.gov/index.html>

*OnGuard Online: U.S. Computer Emergency Readiness Team* by Federal Trade Commission

<http://www.onguardonline.gov/certtips/index.html>

*Operation Blue Ridge Thunder* by Bedford County Sheriff's Office

<http://www.blueridgethunder.com/default.htm>

*ProtectKids.com* by Enough Is Enough

<http://www.protectkids.com/>

*SafeKids.Com*

<http://www.safekids.com/>

*Safe Surfin' Foundation Home Page*

<http://www.safesurfincentral.org/>

*Staysafe.org Home Page*

<http://www.msn.staysafeonline.com/>

*Virginia Center for School Safety* by Virginia Department of Criminal Justice Services

<http://www.dcjs.virginia.gov/vcss/?menuLevel=5>

*Web Wise Kids Home Page* by Web Wise Kids

<http://www.wiredwithwisdom.org/>

*WiredSafety.org* by WiredKids (includes *Teenangels*, *WiredSafety*, and *WiredKids*)

<http://www.wiredsafety.org/>

## **Internet Benefits and Risks**

*Cybercrime Newsletter* by National Association of Attorneys General

<http://naag.org/publications/cybercrime/index.php>

- Online articles about different aspects of *cybercrime*

*GetNetWise: What are the Risks for Children Online?* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/danger/>

- Overview of various Internet risks

*Parenting Online* by WiredKids

<http://wiredkids.org/parents/parentingonline/index.html>

<http://wiredkids.org/resources/documents/pdf/parentingonline.pdf> (Printable version)

<http://www.wiredkids.org/parents/parentingonline/parentingonline-ES-v1.pdf> (Spanish version)

- Internet positives and negatives, plus tips for avoiding problems

“The Positives and Perils of the Internet: Working Together to Make Your Family’s Online Experience Safe and Fun” by Donna Rice Hughes (*ProtectKids.com*)

[http://www.protectkids.com/parentsafety/positive\\_peril.htm](http://www.protectkids.com/parentsafety/positive_peril.htm)

- Safety tips for parents and children

*What Are the Risks* by SafeKids.Com

<http://www.safekids.com/risks.htm>

- Brief overview of potential risks

### **Legal: National**

*Class Action: Virginia Students and the Law* by Attorney General of Virginia

[http://www.oag.state.va.us/KEY\\_ISSUES/CLASS\\_ACTION/](http://www.oag.state.va.us/KEY_ISSUES/CLASS_ACTION/)

- Information about computer crimes (material implemented generally by school resource officers)

*Education Law Association Home Page*

<http://www.educationlaw.org/>

- Developed by educational and legal scholars

*Internet Safety Policies and CIPA: An E-Rate Primer for Schools and Libraries* by E-Rate Central

[http://www.e-ratecentral.com/CIPA/cipa\\_policy\\_primer.pdf](http://www.e-ratecentral.com/CIPA/cipa_policy_primer.pdf)

- Requirements for federal funding related to the Children's Internet Protection Act (CIPA) and Neighborhood Children's Internet Protection Act (NCIPA)

*School Law in Review 2006* by National School Boards Association

[https://secure.nsb.org/pubs/item\\_info.cfm?ID=727](https://secure.nsb.org/pubs/item_info.cfm?ID=727)

- CD-ROM, available for purchase, including most aspects of education law

*School Law: Technology* by National School Boards Association

<http://www.nsb.org/site/page.asp?TRACKID=&CID=397&DID=8638>

- Legal technology information, including resources, news, and recent cases

*SPAM/Technology Crimes: Computer Crime Unit* by Attorney General of Virginia

<http://www.oag.state.va.us/CONSUMER/SPAM/index.html>

- Overview of *cybercrimes* in the Commonwealth of Virginia

*THOMAS* by Library of Congress

<http://thomas.loc.gov/>

- Web site of Congress, including searchable database of *cybercrime* laws

*U.S. Code Collection* by Cornell Law School

<http://www4.law.cornell.edu/uscode/html/uscode20/>

- Past and current U.S. Code chapters related to education, including *cybercrime* issues

*Virginia Department of Criminal Justice Services* by Virginia Center for School Safety

<http://www.dcjs.virginia.gov/vcss/>

- Virginia legislative mandates for school safety

### **Legal: Virginia Laws**

*Computer fraud*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.3> § 18.2-152.3

*Computer invasion of privacy*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.5> § 18.2-152.5

*Computer trespass (hacking/cracking)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.4> § 18.2-152.4

*Enhanced penalties for using a computer in certain violations (advertising/producing obscene materials)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-376.1> § 18.2-376.1

*Harassment by computer (cyberbullying)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.7C1> § 18.2-152.7:1

*Identity theft*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-186.3> § 18.2-186.3

*Personal trespass by computer*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.7> § 18.2-152.7

*Possession of child pornography*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-374.1C1> § 18.2-374.1:1

*Production, publication, sale, possession with intent to distribute, financing, etc., of sexually explicit items involving children*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-374.1> § 18.2-374.1

*Property capable of embezzlement (by computer)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.8> § 18.2-152.8

*Theft of computer services (WiFi surfing)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.6> § 18.2-152.6

*Transmission of unsolicited bulk electronic mail (spam)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.3C1> § 18.2-152.3:1

*Use of communications systems to facilitate certain offenses involving children (solicitation)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-374.3> § 18.2-374.3

*Using a computer to gather identifying information (phishing/pharming)*

<http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.5C1> § 18.2-152.5:1

### **Newsletters**

*FamilyTechTalk* by Larry Magid and Anne Collier (weekly podcasts)

<http://www.familytechtalk.com/>

*GetNetWise-News* by GetNetWise

<http://www.getnetwise.com/news/>

*i-SAFE Times, i-EDUCATOR Times, and i-PARENT Times* by i-SAFE

[http://www.isafe.org/channels/sub.php?ch=op&sub\\_id=4](http://www.isafe.org/channels/sub.php?ch=op&sub_id=4)

*Microsoft Security Newsletter for Home Users* by Microsoft

<http://www.microsoft.com/athome/security/secnews/default.aspx>

*Net Family News*

<http://netfamilynews.org/letterindex4.html>

*Netsmartz Bulletin* by National Center for Missing & Exploited Children and Boys & Girls Clubs of America

<http://www.netsmartz.org/feedback/bulletin.htm>

*OnGuard Online: US-CERT Alerts* by Federal Trade Commission

<http://onguardonline.gov/certalerts.html>

### **Online Games**

*Ready, set, game: Learn how to keep video gaming safe and fun* by Microsoft

<http://www.microsoft.com/athome/security/children/gamingonline.aspx>

- Tips for parents to help children “play it safe with online games”

“10 Tips for Dealing with Game Cyberbullies and Grieferers” on *Ready, set, game: Learn how to keep video gaming safe and fun* by Microsoft

<http://www.microsoft.com/athome/security/children/grieferers.aspx>

- Suggestions for handling *grieferers*, who cause trouble for other online game players

### **Parent/Child Sample Agreements**

*Family Contract for Online Safety* by SafeKids.com

<http://www.safekids.com/contract.htm>

- Kid’s Pledge and Parent’s Pledge

*Kids’ Rules for Online Safety* by SafeKids.com

<http://www.safekids.com/kidsrules.htm>

- Clear list of commitments

*Roos ‘N Tools Youth Pledge* by ProtectKids.com

<http://www.protectkids.com/parentsafety/pledge.htm>

- Family Internet safety contract

*Using family contracts to help protect your kids online* by Microsoft

<http://www.microsoft.com/athome/security/children/famwebrules.aspx>

- Sample contract for online code of conduct

*Web Wise Kids: Internet Safety Plan* by WiredWithWisdom

<http://www.wiredwithwisdom.org/internet-safety-plan.pdf>

- Formatted as, “If [blank] happens, I will [blank]”

### **Peer to Peer (P2P) or File Sharing**

*OnGuard Online: Peer to Peer File-Sharing* by Federal Trade Commission

<http://onguardonline.gov/p2p.html>

- Facts and issues involved with *P2P*

*Sorted: File Sharing* by ChildNet International

<http://www.childnet-int.org/sorted/filessharing.aspx>

- Information on copyright and other legal issues related to *file sharing*

*Young People, Music & the Internet* by ChildNet International

<http://www.childnet-int.org/music/>

- Information and frequently asked questions for parents and young people
- Predators (Including Information on Luring and Grooming)**
- “How to recognize ‘grooming’: Teach your kids” by Anne Collier (*BlogSafety* by Tech Parenting Group)  
<http://www.blogsafety.com/thread.jspa?threadID=120000033>
- Tactics and links to other resources
- Online predators: What you can do to minimize the risk* by Microsoft  
<http://www.microsoft.com/athome/security/children/kidpred.msp>
- Information on how predators work, tips for parents, and guidelines for children
- Predator Tip Sheet* by i-SAFE  
[http://xblock.isafe.org/docs/Eluding\\_Internet\\_Predators\\_Tip\\_Sheet.pdf](http://xblock.isafe.org/docs/Eluding_Internet_Predators_Tip_Sheet.pdf)
- Tips and reminders for recognizing potential problems
- Professional Development**
- i-LEARN* by i-SAFE  
<http://ilearn.isafe.org/>
- Free training with online video modules and lesson plans; requires login ID
- K-12 Professional Development and Overview Presentation* by CyberSmart  
<http://www.cybersmart.org/pd/>  
[http://www.cybersmart.org/info/overview\\_pres.asp](http://www.cybersmart.org/info/overview_pres.asp)
- Free online course for groups of 25 or more
- Reporting Problems**
- Cyberstalking, Harassment, and Cyberbullying Form* by Wired Safety  
<https://www.wiredsafety.org/forms/stalking.html>
- Online form for reporting *cyberstalking* and *cyberbullying*
- TheCyberTipline* by National Center for Missing & Exploited Children  
<http://www.cybertipline.com/>
- Reporting mechanism for child sexual exploitation
- GetNetWise: Reporting Trouble* by Internet Education Foundation  
<http://kids.getnetwise.org/trouble/>  
<http://onguardonline.gov/filecomplaint.html>
- Identifying, reporting, and educating children about online crimes
- Internet Crime Complaint Center* by FBI and National White Collar Crime Center  
<http://www.ic3.gov/>
- Mechanism for reporting and investigating online crimes
- OnGuard Online: File a Complaint* by Federal Trade Commission  
<http://onguardonline.gov/filecomplaint.html>
- Types of online crimes and who should be notified
- Report a CyberCrime* by ProtectKids.com  
<http://www.protectkids.com/report/index.htm>
- Cyber tipline and links to local FBI offices
- Research**
- Online Victimization: A Report on the Nation’s Youth* by Center for Missing & Exploited Children  
[http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en\\_US&PageId=869](http://www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en_US&PageId=869)
- Documentation of youth exposure to sexual solicitation, sexual material, and harassment
- Safe & Smart: Research and Guidelines for Children’s Use of the Internet* by National School Boards Foundation  
<http://www.nsb.org/safe-smart/index.html>
- Suggestions for using the Internet as a positive force
- Statistics: Teen Internet Safety* by National Center for Missing & Exploited Children (commissioned by Cox Communications)  
<http://www.netsmartz.org/safety/statistics.htm>
- Risks and opportunities of teen Internet use
- Study of Entertainment Media & Health: Internet* by Kaiser Family Foundation  
<http://www.kff.org/entmedia/internet.cfm>
- Two reports: (1) Internet use by young people in grades 3-12 and (2) online food advertising that targets children

## Sample School and Division Policies

Andover (Mass.) Public Schools

[http://www.aps1.net/Internet%20Safety/internet\\_safety.htm](http://www.aps1.net/Internet%20Safety/internet_safety.htm)

- Internet safety Web page

Dedham (Mass.) Schools

[http://www.dedham.k12.ma.us/technology/Internet\\_Safety\\_Policy.pdf](http://www.dedham.k12.ma.us/technology/Internet_Safety_Policy.pdf)

- Internet safety policy, pertaining primarily to filtering and monitoring

Geneva (Ohio) Area City Schools

<http://www.genevaschools.org/aup/>

- Acceptable use and Internet safety policy

Henrico County (Va.) Public Schools

[http://www.henrico.k12.va.us/pdf/technology/accept\\_use2005.pdf](http://www.henrico.k12.va.us/pdf/technology/accept_use2005.pdf)

<http://www.henrico.k12.va.us/administration/instruction/technology/safety.html>

- Acceptable use and Internet safety policy

- *Internet Safety* Web page

Lake Washington (Wash.) School District

<http://www.lkwash.wednet.edu/lwsd/pdf/InternetSafetyPolicy.pdf>

- Internet safety policy

Montgomery County (Md.) Public Schools

<http://www.mcps.k12.md.us/info/cipa/index.shtm>

- *Using the Internet Safely for Educational Purposes* Web page, including links to Internet safety and acceptable use policies

Portland (Maine) Public Schools

<http://www.portlandschools.org/CTS/documents/posterSAUP.pdf>

- Student acceptable use and internet safety policy

## Sites for Educators

*Computer Security Resource Center* by National Institute of Standards and Technology, Computer Security Division

<http://csrc.nist.gov/>

- Resources on security tools and practices

CSIA Policy Papers by Cyber Security Industry Alliance

[https://www.csialliance.org/publications/csia\\_whitepapers/](https://www.csialliance.org/publications/csia_whitepapers/)

- Various issues related to *cybersecurity*, including Talking Points For Cyber Security

*Cyberethics for Teachers: A Lesson Plan Outline for Elementary and Middle School Divisions* by U.S. Department of Justice

<http://www.cybercrime.gov/rules/lessonplan1.htm>

- Lesson plan that defines and explains how to prevent computer crimes

*Cyber Security Basics: Consumers* by National Cyber Security Alliance

<http://www.staysafeonline.info/basics/consumers.html>

- Resources to protect the home from cyber threats

*Cyber Security Basics: Educators* by National Cyber Security Alliance

<http://www.staysafeonline.info/basics/educators.html>

- Resources to help students become better cyber citizens

*Cyber Security Basics: Help Keep Kids Connected and Protected* by National Cyber Security Alliance

<http://www.staysafeonline.org/connectedandprotected.html>

- Information for educators and parents about social networking

*Cyber Security for the Digital District* by Consortium for School Networking

<http://securedistrict.cosn.org/>

- Security issues superintendents need to know

*Cyber Security for the Digital District: Understanding the Issues: The K-12 Technology Context* by Consortium for School Networking

<http://securedistrict.cosn.org/admin/issue/context.html>

- Far-ranging paper for district superintendents about various security concerns, including student safety

*Cybersecurity* by EDUCAUSE

[http://www.educause.edu/Browse/645?PARENT\\_ID=702](http://www.educause.edu/Browse/645?PARENT_ID=702)

- Resources that target primarily higher education but also useful to K-12 administrators  
*How to Protect Kids' Privacy Online: A Guide for Teachers* by Federal Trade Commission  
<http://www.ftc.gov/bcp/online/pubs/online/teachers.pdf>
  - Impact of the federal Children's Online Privacy Protection Act on Web site operators and teachers  
*OnGuard Online: Videos and Tutorials* by Federal Trade Commission  
<http://onguardonline.gov/tutorials/index.html>
  - Practical tips about cybersecurity  
"ONLINE SAFETY: What the Children's Internet Protection Act has in store for you this fall" by Elliott Levine (*Electronic School*, National School Boards Association)  
<http://www.electronic-school.com/2001/09/0901onlinesafety.html>
  - Information about developing an Internet safety policy and using filters  
*Play It Cyber Safe* by Business Software Alliance  
<http://www.playitcybersafe.com/resources/index.cfm>
  - Resources for teachers and parents  
*Safe and Secure?* by Scholastic  
<http://content.scholastic.com/browse/article.jsp?id=127>
  - Steps for determining network security  
*Safe & Smart: Research and Guidelines for Children's Use of the Internet* by National School Boards Foundation  
<http://www.nsb.org/safe-smart/index.html>
  - Suggestions for using the Internet as a positive force  
*Safeguarding Your Technology* by U.S. Department of Education, National Center for Education Statistics  
<http://nces.ed.gov/pubs98/safetech/>
  - Guidelines for administrators to secure computer information, software, and equipment  
*US-CERT: U.S. Computer Emergency Readiness Team*  
<http://www.uscert.gov/>
  - Up-to-date information about threats to *cybersecurity*  
*Virginia Alliance for Secure Computing and Networking*  
<http://vascan.org/>
  - Targeted for Virginia higher-education IT security experts, but also helpful to K-12 IT security officials  
*WiredKids: Educators* by WiredKids  
<http://www.wiredkids.org/educators/index.html>
  - Articles for educators, including "Internet Problem Issues for Schools" and "Teacher Safety"
- Sites for Kids**
- Are You a Safe Cybersurfer?* by Federal Trade Commission  
<http://www.ftc.gov/bcp/online/edcams/infosecurity/forkids.html>
  - Online quiz for kids, with printable stickers, posters, and bookmarks  
*Copyright Kids!* by Copyright Society of the U.S.A.  
<http://www.copyrightkids.org/>
  - Information about copyright for students, parents, and children  
*Cyberethics for Kids* by U.S. Department of Justice  
<http://www.cybercrime.gov/rules/kidinternet.htm>
  - Rules for using the Internet and information about hacking  
*CyberSpacers* sponsored by U.S. Department of Justice, Dell, and Information Technology Association of America  
<http://www.cyberspacers.com/>
  - Games, comics, and celebrity interviews focusing on cyberethics issues  
*Cybertreehouse* by Business Software Alliance  
<http://www.cybertreehouse.com/>
  - Information about cyberethics  
*FauxPaw the Techno Cat* by iKeepSafe Coalition  
[http://ikeepsafe.org/iksc\\_statemessage/state.php?abbr=VA](http://ikeepsafe.org/iksc_statemessage/state.php?abbr=VA)
  - Animated movie and book on the left-side menu relate the adventures of a cat in cyberspace  
*Get Your Web License* by PBS KIDS  
<http://pbskids.org/license/>

- Interactive quiz on Internet safety  
*GetNetWise: Safety Tips for Kids* by Internet Education Foundation  
<http://kids.getnetwise.org/safetyguide/kids>
  - Guidelines for Internet safety  
*KidzPrivacy: Just for Kidz* by Federal Trade Commission  
<http://www.ftc.gov/bcp/online/edcams/kidzprivacy/kidz.htm>
  - Information about surfing, privacy, and personal information  
*NetSmartzKids*  
<http://www.netsmartzkids.org/indexfl.htm>
  - Cartoon characters, games, music videos, and e-cards related to Internet safety  
*Problem Solver: Stay Safe Online* by National Crime Prevention Council  
<http://www.mcgruff.org/ProblemSolver/webSafety.htm>
  - Rules, pledge, quiz, activities about Internet safety  
*Safety Tips: Internet Safety* by FBI Kids  
<http://www.fbi.gov/kids/k5th/safety2.htm>
  - Concise overview of cyberethics  
*Sophia's Safe Surfing Club* by WiredKids  
[http://www.wiredkids.org/ktt\\_universal/games/sophia/sophie1.html](http://www.wiredkids.org/ktt_universal/games/sophia/sophie1.html)
  - Information and quiz regarding Internet safety, including a printable Internet Safe Surfing Permit  
*staysafe.org for Kids*  
<http://www.msn.staysafeonline.com/kids/default.html>
  - Activities and games about Internet safety and an explanation of a virtual community  
*Surf Swell Island: Adventures in Internet Safety* by Disney  
<http://disney.go.com/surfswell/index.html>
  - Fun activity site, with many ads  
*Web Literacy Tips* by PBS KIDS  
<http://pbskids.org/privacy/literacytips.html>
  - Concise, simple language kids can understand  
*Web Wise Kids: Safety Tips for Kids* by WiredWithWisdom  
<http://www.wiredwithwisdom.org/internet-safety-tips-kids.pdf>
  - Short list of do's and don't's
- Sites for Older Kids**
- *Computer Security Awareness Video Contest* by EDUCAUSE  
<http://www.educause.edu/SecurityVideoContest/7103>
  - Online prize-winning videos by college students  
*Don't Believe the Type* by NetSmartz  
<http://tcs.cybertipline.com/>
  - Links to "Know the Dangers," including tips for keeping safe with various technologies  
*GetNetWise: Safety Tips for Teens* by Internet Education Foundation  
<http://kids.getnetwise.org/safetyguide/teens>
  - Guidelines for online communications  
*Internet Superheroes* by WiredKids  
<http://www.internetsuperheroes.org/>
  - Internet safety/security issues, such as cyberbullying and instant messaging, using Marvel superheroes  
*SafeTeens.Com* by SafeKids.Com and Internet Safety Project  
<http://www.safeteens.com/>
  - Common sense advice on newer technologies  
*staysafe.org for Teens* by staysafe.org  
<http://www.msn.staysafeonline.com/teens/default.html>
  - Straightforward articles about various technologies and how to enjoy the Internet, stay safe, and communicate with parents  
*Teenangels* by WiredSafety  
<http://www.teenangels.org/>
  - Specially trained teens who spread the word in their schools about Internet safety  
*X-BLOCK: i-MENTORS* by i-SAFE  
<http://xblock.isafe.org/imentors.php>

- Free online training for students (grades 5-12) to become i-MENTORs and promote Internet safety at school

### **Sites for Parents**

*Cyber Security Basics: Consumers* by National Cyber Security Alliance

<http://www.staysafeonline.info/basics/consumers.html>

- Resources related to Internet security

*Cyber Security Basics: Family & Children* by National Cyber Security Alliance

<http://www.staysafeonline.info/basics/family.html>

- Resources for parents to protect children

*Cyber Security Basics: Help Keep Kids Connected and Protected* by National Cyber Security Alliance

<http://staysafeonline.org/connectedandprotected.html>

- Guide for educators, parents, and guardians regarding social networking sites

*Don't Believe the Type: For Parents and Guardians* by NetSmartz

<http://tcs.cybertipline.com/parentsguardians.htm>

- Tips for parents to keep their teens safe

*GetNetWise: Safety Tips for Families* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/families>

- Guidelines for protecting children

*How to Protect Kids' Privacy Online* by Federal Trade Commission

<http://www.ftc.gov/bcp/online/pubs/online/kidsprivacy.pdf>

- Impact of the federal Children's Online Privacy Protection Act on Web site operators and parents

*Internet Safety: Information for Parents* by WiredKids

<http://www.wiredsafety.org/parent.html>

- Frequently asked questions by parents, including many related to new technologies

*i-PARENT* by i-SAFE

<http://ilearn.isafe.org/>

- Free online training modules help parents protect their children

*Keeping Children Safe Online* by U.S. Computer Emergency Response Team

<http://www.us-cert.gov/cas/tips/ST05-002.html>

- Suggestions for parents to protect their children online

*Keeping Your Kids Internet Safe and Smart: A Survival Guide for Parents* by Common Sense Media

<http://www.common sense.com/download/index.php>

- Free downloadable booklet and weekly e-mail updates

"My Turn: There's One More Talk You Need to Have" by Martha Stansell-Gamm (*Newsweek*, September 15, 2003)

<http://www.cybercrime.gov/onemoretalk.htm>

- Short article by the head of the U.S. Department of Justice's Computer Crime and Intellectual

Property Section

*A Parent's Guide to Internet Safety* by FBI

<http://www.fbi.gov/publications/pguide/pguidee.htm>

- Detailed publication, including tips and definitions

*A Parent's Guide to Online Kids* by The Children's Partnership

[http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches\\_and\\_Presentations&CONTENTID=9071&TEMPLATE=/CM/ContentDisplay.cfm](http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches_and_Presentations&CONTENTID=9071&TEMPLATE=/CM/ContentDisplay.cfm)

- Online PowerPoint presentation covering various types of Internet access and potential benefits/dangers parents should know

*The Parent's Guide to the Information Superhighway: Rules and Tools for Families Online* by The Children's Partnership

[http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches\\_and\\_Presentations&CONTENTID=4687&TEMPLATE=/CM/HTMLDisplay.cfm](http://www.childrenspartnership.org/AM/Template.cfm?Section=Speeches_and_Presentations&CONTENTID=4687&TEMPLATE=/CM/HTMLDisplay.cfm)

- Downloadable PDF guide, published in 1998 but still provides useful information about children and the Internet

*Parent's Rules 'N Tools* by ProtectKids.com

<http://www.protectkids.com/parentsafety/index.htm>

- Guidelines for parents in protecting their children

*Raising CyberSafe Kids* by National Crime Prevention Council

<http://www.mcgruff.org/Grownups/is.htm>

- Overview of dangers and how to protect kids

*Safe Surfin' Foundation*

<http://www.safesurfincentral.org/>

- Resources on educating young people about Internet crimes

*Social Networking Sites: A Parent's Guide* by Federal Trade Commission

<http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec13.pdf>

- Tips for protecting children

*staysafe.org for Parents* by staysafe.org

<http://www.msn.staysafeonline.com/parents/default.html>

- Articles explaining newer technologies, communication and safety issues, and practical tips for using software to keep children safe

*10 Common Questions about Internet Safety* by iKeepSafe.org and Symantec

[http://www.ikeepsafe.org/iksc\\_partners/symantec/](http://www.ikeepsafe.org/iksc_partners/symantec/)

- Free online "Parent's Tech Tutorial"

*Web Wise Kids: Tips for Parents* by WiredWithWisdom

<http://www.wiredwithwisdom.org/internet-safety-tips-parents.pdf>

- List of recommendations for parents

*Web Wise Kids: Wired with Wisdom* by WiredWithWisdom(Online or CD course, fee)

<http://www.wiredwithwisdom.org/wiredwithwisdom.asp>

- Tutorial for parents on how to keep their children safe on the Internet; CD or downloadable for fee

*WiredKids: Parents* by WiredKids

<http://www.wiredkids.org/parents/index.html>

- Resources available under "Parent" pull-down menu

*Yahooligans! Parents's Guide* by Yahoo!

<http://yahooligans.yahoo.com/docs/safety/index.html>

- Safe-surfing guidelines

*Yahooligans! Parent's Guide to Internet Rating Systems* by Yahoo!

[http://yahooligans.yahoo.com/Parents\\_\\_Guide/Safety\\_Sites/Rating\\_Systems/](http://yahooligans.yahoo.com/Parents__Guide/Safety_Sites/Rating_Systems/)

- Links for parents

### **Social Networking (Blogs, Personal Web Pages, Chats)**

*Blogsafety* by Childnet International

<http://www.childnet-int.org/blogsafety/>

- Excellent site with advice for all stakeholders

*BlogSafety Forum* by Tech Parenting Group

<http://www.blogsafety.com/>

- Information for kids, parents, and teachers about how to use blogs safely, including acronyms

*ChatDanger: How to Keep SAFE While Chatting Online* by Childnet International

<http://www.chatdanger.com/>

- Social networking true stories

*GetNetWise: Chat* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/technology/chat>

- Suggestions for avoiding problems in chat rooms

*GetNetWise: Social Networking Sites* by Internet Education Foundation

<http://kids.getnetwise.org/safetyguide/technology/socialnetworking>

- Suggestions for parents and children

*Social Networking Sites: Safety Tips for Tweens and Teens* by Federal Trade Commission

<http://www.ftc.gov/bcp/edu/pubs/consumer/tech/tec14.pdf>

- Tips for socializing safely online

*Tips for Safer Chatting* by Microsoft

<http://www.microsoft.com/athome/security/online/chatsafety.msp>

- Recommendations for both parents and kids

### **Student Instruction: Lesson Plans/Curricula**

*Activities and Lessons* by Wired Safety

# APPENDIX

## \*B\*

# Internet Safety Resources





<http://daol.aol.com/safetycenter/parentalcontrols>

Discover AOL

AOL SEARCH

Search

MAIN SAFETY & SECURITY COMMUNICATION CONVENIENCE INFO & ENTERTAINMENT PARENTS CENTRAL

# AOL Safety and Security Center

- ▶ Main
- ▶ Virus Protection
- ▶ Spyware Protection
- ▶ Firewall
- ▶ Phishing Protection
- ▶ Parental Controls
- ▶ Spam Protection
- ▶ Web Pop-Up Controls
- ▶ Safe Surfing

## AOL Parental Controls Are Now Available for Free to Everyone

Once you have an AOL.com email address, it takes just a few easy steps to set up an age-appropriate experience for your child. **When you set up Parental Controls, you can:**

- ▶ Control which Web sites your child can visit
- ▶ Decide who can communicate with your child via email and instant messages
- ▶ Receive email "report cards" of a child's online activity
- ▶ Decide when and for how long your child can be online

### Ready to Set It Up? Here's What to Do:

- 1** Set up an AOL.com email address (screen name) for your children. You can add up to **six** AOL screen names under your own screen name, all for free, each with its own age-appropriate access level (kids only, young teen, mature teen).
- 2** Download and install **Internet Access Controls** on each computer that your child will be using. This feature is required to enforce Parental Controls when your child is using Microsoft® Internet Explorer or another Web browser. Once this feature is installed, everyone who uses **this computer** must sign in to AOL before using any Internet program.
- 3** Go to <http://parentalcontrols.aol.com> to change parental-control settings for each screen name (**optional step**).



## AOL Tools

### **AGE APPROPRIATE CONTENT:**

Selecting from the relevant age category for a child serves to that child only age appropriate content ranging from filtered search results and monitored message boards, to age-appropriate music, movie clips and video games.

### **E-MAIL CONTROLS:**

Allows parents to block specific senders and even filter out spam that may contain inappropriate content.

### **GUARDIAN REPORTS:**

Guardian Reports provide a list of every Web site their child visit on the AOL (and the rest of the Internet if IAC is installed) which sites are blocked from them and how many e-mails and IMs they send and receive and from whom every time they sign on.

### **WEB CONTROLS:**

AOL automatically blocks all children from viewing sites that may contain inappropriate content based on their age. The Web-Unlock feature also allows parents to restrict or allow a specific web just for their child.

### **IM AND CHAT CONTROLS:**

Parents can decide who can send their child instant messages, and whether or not they can use enhanced features like video, voice and file sharing-over-IM. Parents can limit children to chat rooms that are 100% monitored on AOL.

### **ONLINE TIMER:**

Allows parents to control the amount of time, hours during the day or even days of the week that a child can go online.

### **INTERNET ACCESS CONTROLS:**

Extends Parental Controls beyond the AOL client and reaches the rest of the Internet applications on a pc. Once this feature is installed, everyone who uses this computer must sign in to AOL before using any Internet program.



## Useful Links and Resources

[NetSmartz](#) & [Corporate Partner Safety Programs and Materials](#) (NCMEC)



[BlogSafety Community: BlogSafety Forum](#)



[Enough is Enough: Protecting our Children Online](#)



[ProtectKids.com](#)



[Welcome to Safety Clicks!](#)



[GetNetWise | You're one click away](#)



[staysafe.org](#)



[Net Family News - kid tech news for parents](#)



[SafeKids.com Home Page](#)



[SafeTeens.Com Home Page](#)





## Protecting Children Online

Google is deeply committed to protecting children on the Internet and providing all of our users with a safe experience. Our approach has three primary elements: (1) powerful tools to empower families to control their activity online; (2) cooperation with law enforcement and industry partners to stop illegal content and activity online; and (3) educational efforts to increase awareness about online safety. We're pursuing this approach through a number of initiatives:



- **SafeSearch tool for users to filter unwanted content.** We understand that many people prefer not to have adult content included in their search results, especially when children are using the computer. Google has developed its own SafeSearch filter, which uses advanced technology to block pornographic and explicit content from search results. Users can customize their SafeSearch settings by clicking on the "Preferences" link to the right of the search box on Google.com.

- **Cooperation with law enforcement to combat child exploitation.** Google responds to thousands of law enforcement requests for assistance each year and has a legal team devoted to this effort 24 hours a day. We respond to hundreds of subpoenas a year as part of our cooperation in local and federal child safety investigations.



- **Strict prohibition on illegal content in our products.** For example, our AdWords program has a strict policy prohibiting advertising that promotes child pornography or other illegal material, and all ads are reviewed to ensure their compliance with this policy. We invite our users to tell us about illegal content they encounter on the Web through the Google Help Center. When we discover child pornography or are made aware of it, we respond quickly to remove and report it to NCMEC.



- **Engagement in industry-led efforts to fight child pornography.** Google is working with coalitions of financial and technology companies and NCMEC to develop new solutions aimed at eradicating child pornography on the Internet.

- **Support for educational efforts to increase awareness about child safety online.** For example, Google is working with the National Center for Missing and Exploited Children (NCMEC) to run an online advertising campaign promoting resources for reporting child exploitation and educating users about online safety. Google is also supporting the efforts of WiredSafety to provide community officers with training materials for use in schools and sponsored a WiredSafety Internet Safety Summit focused on best practices for social networking websites.



For more information about Google's efforts to protect children online, please contact:

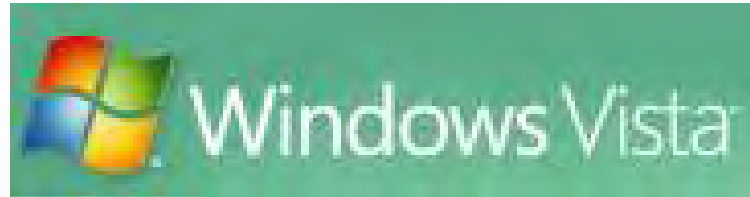
Alan Davidson

Washington Policy Counsel, Google Inc.

202.742.6522

[adavidson@google.com](mailto:adavidson@google.com)

# Microsoft Online Safety Tools and Resources



**After extensive communication with parents, who told Microsoft that in addition to education and guidance, they want technology that can help make their children's online experiences more secure, Microsoft created the following:**

## **Windows Vista**

We've built a parental control platform into Windows Vista, so parents can feel confident that their children are safe when they are working with their PCs. All your applications can plug into this platform, including instant messaging, browsing and gaming. Parents will be able to monitor and restrict when and for how long children can log on, which Web sites they browse on Windows Internet Explorer 7, and what applications they can run.

## **Windows Live Family Safety Settings**

Formerly known as Parental Controls, Family Safety Settings is a free Web-based service that will aid parents in providing a safer experience for their children online by helping block inappropriate content and facilitating safer online communication. Family Safety Settings will offer customizable content filters that will block inappropriate content, a kids request line, reporting features and a contact list management tool, all of which allow parents to set standards for the types of sites that kids and family members can visit. Most important, Family Safety Settings is user-based, not PC-based, so the settings applied to each family member's account will remain intact anytime they log onto a PC equipped with Family Safety Settings software. The service will launch through a phased rollout beginning in 2006.



## Windows Live OneCare

Is a comprehensive, automatic and self-updating PC care service that continually manages vital computer tasks so people don't have to worry about protecting and maintaining their computers. Windows Live OneCare is:

- Comprehensive:** Delivers up-to-date security, recommended PC maintenance for optimal performance, and backup and restore of your important files and photos
- Automatic:** Works continuously 24x7 to help protect and maintain your PC
- Evolving:** Helps ensure you have the latest technology to protect against new threats
- All-in-one:** A simple solution to own, use and maintain

**MSN** has made a number of investments that will let children use the Internet and help parents' rest easy knowing that they can have a safer and more secure experience online.

**Premium Parental Controls** offers parents the ability to restrict their children's access to the Internet, MSN services and who they contact. Parents can also sign up for a weekly activity report displaying the URLs visited, e-mails sent and received, IM contacts and other activities performed online.



**MSN Spaces**, an Internet communications service designed for ages 14 and older, provides customers with the choice of keeping their Space private or public, and MSN Spaces Code of Conduct specifically prohibits any activity harmful to minors. Later this year, Family Safety Settings' contact list management feature will help families manage who their children contact and who contacts them via their Space.

**MSN Kids Channel** offers Internet programming just for kids with activities tailored for specific ages.



**MSN Kids Safe Web Search** offers up search results that are targeted for children. A child can also click on a category, such as School and Homework, and bring up sites such as KidsConnect, hosted by the American Library Association.

**MSN Chat Service** can only be used if the customer is over 18, has a credit card and signs up for the entire MSN subscription service.



**Xbox** strives to provide a safe, secure environment and age-appropriate content for all users; this has been a part of the Xbox story from the very beginning. As an industry leader, Microsoft is committed to helping create an environment in which all users can securely enjoy the full benefits of interactive entertainment. Microsoft does this by including the following safety features:

Xbox parental controls give parents the ability to decide within what parameters their child can use the Xbox console.

Xbox 360 Family Safety Settings allow parents to customize their children's playing environment.

Xbox 360 recognizes games rating from countries around the world, allowing parents to decide what level games they want their children to play.

## **For additional information on other online safety curriculum and programs go to:**

[www.microsoft.com/protect](http://www.microsoft.com/protect)



[www.staysafe.org](http://www.staysafe.org)



[www.ilearn.isafe.org](http://www.ilearn.isafe.org) (training and content for K-12 educators, parents, 50+). Content provided free to partners: PSA's, scripted presentations, brochures, fact sheets, flyers.

[www.staysafe.org/getnetsafetour/default.html](http://www.staysafe.org/getnetsafetour/default.html) -- "Get Net Safe Tour." The Get Net Safe Tour is a national 12-city tour and joint initiative between partners in government, non-government and Microsoft designed to raise consumers' awareness of computing security and Internet Safety so they can help better protect their PC's, their information and their families.



### **MySpace Safety and Security Overview**

MySpace is committed to making our community as safe as possible for all of our members. Safety and security are built into every new site feature and we have designed and built features specifically to enhance the security of our online community. This is an ongoing process that we are constantly reviewing and updating under the leadership of our Chief Security Officer, Hemanshu Nigam, who spent 16 years as a career prosecutor and child safety advocate.

We have worked hard to make sure that users only have access to age appropriate content, to shield younger users from older members of the community, and to partner with law enforcement as a partner with these efforts. Some of the most significant steps we have taken in this area include:

#### **Protecting Underage Users**

- Our Terms of Service indicate that Users must be 14 yrs of age or older to utilize our site
- We employ a search algorithm, utilizing several thousand terms commonly used by underage users, to seek and weed out individuals misrepresenting their age
- Additionally, our team actively searches out underage users by hand
- We delete 25,000 profiles per week for misrepresenting age

#### **Protecting Younger Users from Inappropriate Contact**

- Users under 16 are automatically assigned a Private Profile
- No user can Browse for users under 16
- Adults can never add under 16's as a friend unless they know the under 16's first/last name or email address
- Mature groups cannot be accessed by under 18's

#### **Protecting Younger Users from Inappropriate Content**

- Known inappropriate URLs are blocked from being posted on site
- All IP logs of image uploads are captured, retained and reported to user
- User accounts deleted for uploading pornographic videos
- Tobacco/Alcohol ads prohibited from reaching under 18's/under 21's
- Smoking/Drinking preferences blocked for under 18's/under 21's
- Every image, group, profile, video, group and classified reviewed by hand, this includes over 7 million images per day



### Reporting Inappropriate Content

- Users can report inappropriate content, behavior to MySpace
- Users can send spam email complaints to MySpace
- Users can directly report sexually explicit conduct to NCMEC's CyberTipLine

### Tools for Members

- All members can set profile to Private
- Users can pre-approve all comments before being posted
- Users can block another user from contacting them
- Users can conceal their 'online now' status
- Users can prevent forwarding of their images to other sites
- 32,000 trained school moderators oversee forums

### Education

- Safety Tips on every page including links to blocking software
- Contact MySpace on every page
- Under 18's must review and agree to Safety Tips upon sign-up
- Links promoting safety on every single MySpace page
- Creation of MySpace Parent Brochure
- Creation of School Administrator's Guide to Understanding MySpace and Social Networking Sites
- Aggressive education campaign through MySpace, News Corp properties, and third-party partners including National Center for Missing & Exploited Children, National PTA, AdCouncil, Seventeen Magazine, National School Board Association & the National Association of Independent Schools.
- Extensive PSA campaigns across News Corp properties
- Partnerships with organizations such as CommonSense Media and WiredSafety.org



### Law Enforcement

- Ongoing support for local, state and federal law enforcement
- 24/7 dedicated hotline created for use by law enforcement – not just for emergencies
- Training cybercrime units on how to investigate and prosecute cyber criminals using MySpace
- Law Enforcement Guide and One Sheet created to help law enforcement agencies understand MySpace and investigate cases

### Taking Ongoing Safety/Security Measures to Spot & Solve Safety Challenges

- Nigam, a former Department of Justice Internet crimes prosecutor who held executive-level security positions at Microsoft and the MPAA, leads a team who work full-time on safety and security-related initiatives
- Rapid Response Team in place for sensitive issues
- Red Team formed to identify policy issues and implement solutions
- Content Assurance Team formed to ensure integrity of safety systems and flag potential flaws

These measures represent just a sampling of the steps MySpace has taken to protect our community's safety and enforce our rules. We look forward to answering any questions you might have and sharing new security initiatives with you on an ongoing basis.



Educational Partnerships





## **Ratings/Filtering/Monitoring**

The Yahoo! network is labeled with Internet Content Rating Association (ICRA) labels. In addition, Yahoo! has incorporated filtering and privacy options into its products, including Instant Messaging (IM), Message Boards, and Search. "Family Accounts" provides parents with safety information during the registration process for children under 13 and allows parents to manage their child's account. Yahoo! also restricts usage of certain services based on users' registered ages. Currently, Yahoo! Chat, 360, Personals and other services are restricted to users who are 18 years of age or older. Yahoo!, in conjunction with our access partners AT&T and Verizon, provides parents with parental control software.

Yahoo! is proactive regarding enforcing our Terms of Service on our network and employs a myriad of techniques, including filters, algorithms, and human review, to detect and remove illegal child pornography. In addition, Yahoo! is a founding member of the Center for Child Protection Technologies, a coalition of major service providers and NCMEC aimed at developing new technologies to detect and report content related to the exploitation of children online.



## **Law Enforcement**

Yahoo! partners closely with law enforcement on investigations to protect children. We have a team in place to handle emergencies 24 hours a day, every day. We provide training materials about the Yahoo! network for law enforcement and regularly participate in law enforcement training events sponsored by Internet Crimes Against Children (ICAC) task forces, the American Prosecutor's Research Institute, and the National Association of Attorneys General. Yahoo! also provides sponsorship for local and national ICAC Conferences and Crimes Against Children Conferences. We are a member of the Financial Coalition Against Child Porn.



### **National Center for Missing and Exploited Children (NCMEC) Support**

Yahoo! is an active partner with NCMEC on child pornography reporting. We adhere to the United States Internet Service Provider's Associations Sound Reporting Practices for reporting child pornography to NCMEC. We also support NCMEC's efforts to assist missing kids by providing geo-targeted Amber Alerts on the Yahoo! network. Since 2002, we have sponsored the Annual Hope Awards and Congressional Breakfast. We also have provided NCMEC with free banner and search marketing advertising to help drive traffic to the NCMEC site and promote awareness of NCMEC safety content.

### **Ikeepsafe.org**

Yahoo! is a "Gold Medal" financial sponsor of Ikeepsafe.org. We also provide sponsorship of the DARE internet safety and the "Train the Trainers" events for DARE officers. Ikeepsafe.org is focused on teaching kids and parents about internet safety through its website, but also by distributing educational materials in schools. It makes online safety information available to teachers for free via download from its website.

