



Protecting Children from Sexual Predators: SB 132
Attorney General Roy Cooper
July 24, 2007

Protecting children from sexual predators requires a comprehensive strategy. Through SB 132, Attorney General Roy Cooper proposes to:

- I. Require social networking websites to get parent's permission before children can join**
- II. Enhance the criminal penalty for solicitation of minors for sex over the Internet when the child predator shows up at a meeting place to carry out the sexual assault on the child**
- III. Ban North Carolina sex offenders from social networking sites and from changing their legal names to avoid detection**
- IV. Strengthen criminal penalties for possession, dissemination and production of child pornography**
- V. Expand North Carolina law regarding child pornography to include indecent child exposure as federal law does**
- VI. Make lying to a State Bureau of Investigation agent a felony**

I. Require social networking websites to get a parent's permission

Social networking sites are the new playground for predators. As of July, 2007, MySpace has found more than 29,000 registered sex offenders on its site, four times more than its original estimate. That number includes just the predators who signed up using their real names, and not the ones who failed to register or used fake names, or who haven't been convicted.

Websites that encourage children to share personal information and to talk online to others offer predators easy targets. Last fall the SBI arrested a North Carolina police officer for raping a 14-year-old girl he had lured through MySpace, a site that hosts detailed profiles of millions of children and adults. Few safeguards keep the children away from adult users, so child users are exposed to adults seeking sex and more.

This proposal requires that these websites get a parent's OK before children under 18 join and post personal information, and give parents the chance to see what their children post.

Parents, educators and law enforcers are worried. They warn kids to be private and stay safe, but see time and again that some children don't know what's OK to share. Parents of victims are often shocked to know their children were using the computer to talk strangers. A Clayton mother writes that several pre-teen girls in her daughter's class are members of the site, despite the rule prohibiting members under 14: "I submitted this information to MySpace, via multiple methods they offer, but the profile remains to list the user as 15, although she just reached her 13th birthday on 13 April 2007."

A review of media reports through the first six months of 2007 found more than 100 criminal incidents involving adults who used MySpace, the largest social networking site, to prey or attempt to prey on children. That's double the number of such incidents reported in the media in 2006. That's only one website, and doesn't include incidents that went unreported.

Cooper and other attorneys general have pushed MySpace to find a way to get parent's approval before children can become a member. It would work by having the site verify a parent's identity; the parent would then decide whether a child could join. A public records database, for example, could establish a parent's identity, and a follow-up phone call or postcard could verify that the parent gave approval. Only with a parent's consent could the child create a personal page for the public to view, posting photos, favorites and friends, and communicating with other members.

By knowing their members' true ages, the online social networking sites would also be able to keep kids from adults and adult content such as pornography, as well as keeping keep predators away from children.

Checking a child's ID is already used for alcohol, tobacco, movies, gambling, and financial institutions. In addition, federal legislation such as the Children Online Privacy Protection Act ("COPPA") has used this model of parental permission with success for the past decade. California and Virginia, have statutes requiring identity verification for online tobacco sales.

II. Enhance the criminal penalty for solicitation of minors for sex over the Internet when the child predator shows up at a meeting place to carry out the sexual assault on the child

The SBI and local law enforcement have had success using our new law that makes it a felony for an Internet predator to solicit a child for sex, including an undercover officer he or she believes to be a child. This law also requires convicted online predators to be added to the state's Sex Offender Registry and to provide DNA samples for the state's convicted offender database.

However, North Carolina should enact a tougher criminal penalty for a predator who solicits a child over the Internet and then follows through by showing up at the meeting place. An example:

Last year, a longtime middle school teacher who also worked as a coach was charged with soliciting a child for sex by computer. The defendant communicated by instant messages, inviting a 15-year-old boy for a sexual encounter. The boy's father found out and told law enforcement, and a deputy posed as the boy to set up a meeting. The offender arrived with lubricant, two condoms and a digital camera. Investigators later found thousands of child porn videos and photos and charged him with 20 counts of second-degree sexual exploitation of a minor.

III. Ban North Carolina sex offenders from social networking sites with child members and from changing their names to avoid detection

More than 29,000 sex offenders nationwide and hundreds in North Carolina alone have joined MySpace, just one of the social networking sites. Under this bill, North Carolina sex offenders would be banned from joining the sites which allow children to become members. The offenders would also be prohibited from changing their legal names in state courts so as to avoid detection on the state Sex Offender Registry maintained by the Department of Justice.

IV. Strengthen criminal penalties for possession, dissemination and production of child pornography

Incidents of child sexual exploitation reported in North Carolina continue to rise. The National Center for Missing and Exploited Children (NCMEC), which tracks online and telephone reports of child solicitations and exploitation, had 11 incidents reported in 2001; in 2005, 252 were reported and in 2006 the number topped 400 (NCMEC, Dec. 7, 2006 YTD).

Law enforcement officers report and a study has shown that child predators often use and distribute child pornography as well. Federal law imposes stronger criminal penalties for the possession, dissemination and production of child pornography than North Carolina currently provides. Possession of child pornography under federal law provides up to 10 years active prison time. Under North Carolina law, possession of child pornography for first-time offenders carries no active prison time.

V. Expand North Carolina law regarding child pornography to include indecent child exposure as federal law does

North Carolina's child pornography statute currently makes it a crime to produce, distribute, or possess material containing "a visual representation of a minor engaged in sexual activity" (NCGS §§ 14-190.16 through 17A). Sexual activity is

defined in section 14-190.13, but does not include the suggestive display of the genital area of the minor. Federal law includes the state definition, but also the "lascivious exhibition of the genitals or pubic area of any person" (18 USCS § 2256) and provides a broader definition thus providing greater protection for our children against those who attempt to sexually exploit them.

V. Make lying to an SBI agent a felony

More than 10,000 convicted sex offenders currently live in North Carolina. Many share pornographic images of children with each other, and those who do often know who the child is and where they live. Making lying to an SBI Agent a felony would provide a critical incentive for sex offenders to tell investigators where the child is so that the SBI can rescue the child and prevent further exploitation.

SBI agents know witnesses withhold information or lie outright. When an FBI agent is present, a dishonest witness can be charged with a crime, since federal law makes it a felony to lie to federal agents.

The SBI handles the state's most complex and challenging felony criminal investigations in North Carolina. This new provision will provide the SBI with a critical investigative tool to compel witnesses to tell the truth. Whether it is a crime of murder, rape, child sexual exploitation, child pornography, or the embezzlement of private or public funds this strong investigative tool will help apprehend perpetrators and provide real penalties for those who deceive.

SB 132: Q&A ON PARENT'S PERMISSION FOR SOCIAL NETWORKING SITES
ATTORNEY GENERAL ROY COOPER
SB 132

Q. What are social networking sites?

A. Social networking websites allow people to become members and share information like photos, favorite songs, hometowns and more. Popular social networking sites include MySpace, Facebook, and Xanga.

Children who join often share personal information with the world, but many companies that operate commercial social networks take little responsibility for monitoring the content or conduct of members.

Many social networks, including MySpace, allow children as young as 14 as well as adults to join and interact with each other, and social networking sites fail to ensure that members disclose their actual age. Adults pose as children and take advantage of honest kids who disclose their real age when becoming a member. Children younger than 14 easily join simply by saying they're 14.

As a result, children have been the targets of sexual predators, scam artists, identity thieves and other criminals. The predators often pretend to be children to lure the child into meetings.

Q. Who would be affected by this bill?

A. The law would apply to all companies that operate a social networking site on the Internet if the site is operated for profit and minors are allowed to be members. It requires companies to get a parent's permission before allowing the child to join.

Q. Would it include auction sites like eBay and Amazon, or photo sharing sites like Kodak Gallery and flickr?

A. No, the bill excludes such sites.

Q. How will sites verify the identity of parents?

A. The bill doesn't mandate a way, though many are available. To help companies comply, the bill provides a safe harbor provision that creates defenses for companies working to obtain parental permission.

Q. Does the technology exist to verify that parents are who they say they are?

A. Yes. The companies can choose a method that works best for them. For example, verification by credit cards, public databases, follow-up questions and other methods can be used.

Today, some companies, such as Anheuser-Busch and its Bud.TV website, use public databases. Others use financial records such as credit cards. For example, Microsoft offers free web hosting services but requires members to provide a valid credit card to join as proof of identity.

Q. What if a child predator pretends to be parent, and then creates an account for a fake teen? Could the predator still pretend to be a teen, and have access to children?

A. Already predators pretend to be kids on social networks and the sites aren't preventing it, which is why North Carolina parents should be given legal authority to prevent their children from becoming a member without their permission.

Requiring validation means the real name of the predator who pretends to be a child will be shared, which is a real deterrent for predators.

Q. Does the identity verification process compromise privacy?

A. Not when it's done right. Social networking sites already solicit personal information from children, sometimes with disastrous consequences. Parental permission would mean that an adult, not the child, would review a company's privacy policy, check its reputation, be sure the site is secure and know where to go for help if there are problems.

In addition, the bill prohibits the companies from using any information provided in the permission process for any purpose other than granting permission.

Q. Will this create information on children that could then be compromised?

A. No. Plus, companies operating social networks already compile information about children by requiring minors to provide information about themselves to become a member.

Once a child becomes a member, the network and other members solicit the child for personal information, which is often shared with all members and non-members. Eliciting private details like school name, grades, interests, hobbies, sexual orientation and latest boyfriends puts children at risk to potential sexual predators. It also makes them susceptible to identify theft, targeted marketing, and more.

Q. Will this be too costly for social networking sites because of the large number of users?

A. While there will be some cost to companies, many sites already absorb this cost with some system of verification. Our children's well-being is worth this minimal investment, particularly when the owners of social networks rely on children becoming members to increase the value of their investment.

By comparison, in 2005 News Corp. paid more than half a billion dollars to purchase MySpace. Google will pay News Corp. \$900 million to provide advertising for three years on MySpace. Recent sales reports place the value of MySpace in the billions.

Q. Is this law Constitutional?

A. We have found no case that tests the constitutionality of parental consent as a condition of membership to a social network. This bill simply requires parental permission, which allows parents to choose if their child joins a website that could be dangerous. It does not regulate the content of anyone's speech.

At the federal level, the Children's Online Privacy and Protection Act, just like SB 132, prevents social networks from collecting personal information from children without parental approval. This law operates in full force and hasn't been declared unconstitutional. In fact, last year one social network, Xanga, paid a \$1 million fine after allowing more than one million children under age 13 to join without parental approval.

North Carolina has other parental permission laws. For example, NCGS §14-400(b) prohibits body piercing of a child under 18 years of age without parental consent. Children younger than 16 cannot be employed by establishments that serve alcohol without their parent's consent. NCGS §95-25.5(j)(1). Schools regularly require students to get their parent's permission before going on a field trip or participating on athletic teams.

Q. How does the site know that an individual is using a computer in North Carolina?

A. Technology can identify a computer's location. This information is used to direct local advertising and other services based on a computer's location. Technology companies have made geographical identification on the Internet reliable and often invisible. These firms analyze Internet Protocol (IP) addresses along with various databases to determine the geographical location of the Internet use with high degree of accuracy.

Many social networks are already checking IP addresses of their members. As the MySpace privacy statement says: "IP addresses are recorded for security and monitoring purposes."

Q. Could parents just block the sites?

A. Blocking and monitoring software are useful tools for parents; however they aren't a complete solution since the software can only help on the computer where it's been installed. Children would still be able to access sites at schools, libraries, their friend's homes, on gaming equipment like Playstation3, or even on their cell phones.

The better solution is to have a parent give permission before his or her child can join a social networking site in addition to having a parent install software on the home computer.

Q. Are public education, better enforcement of existing laws, or more parent involvement better suited to solving this problem?

A. Educating parents and kids about online risks is critical. The Attorney General and his staff have conducted hundreds of seminars around the state for parents and educators on Internet safety. Education is an important part of the effort to protect our children, but it needs to be combined with a law enforcement focus and better safeguards for kids online.

Q. Will this give parents a false sense of security?

A. No more than other efforts to make children safer when using the Internet. For example, some operators of social networks have made improvements to reduce the risks to child members. Last year, MySpace hired its first Chief Security Officer whose responsibility includes user safety. But having a security officer doesn't erase danger, as MySpace recognized in running public service announcements stating that "one in five kids online is sexually solicited."

By requiring parental permission, North Carolina would give parents a legally enforceable right to decide when a child asks "can I be a member of this site where 60 million strangers can contact me?"