Children and Online Sexual Predators.

A sexual predator sits in a chatroom, waiting for the right child to enter. The child does. They always do. Thirteen years old, the young girl chats happily about her school, her softball team and her music. The sexual predator reaches out, "I love ___ [insert her favorite pop star] too!." The young girl bites, and the conversation begins. The sexual predator may be masquerading as a cute fourteen-year-old boy, or another young teen girl. But no matter what persona he takes on, it is with the single goal of meeting this girl offline, for sexual exploitation. And, with between 12% and 24% of the teen girls[1] surveyed admitting to meeting online acquaintances offline, in person, the risk of his being able to succeed is very real.

Those percentages would increase significantly if the predator knew how to contact the child offline and more about who they are and where they live. Information is what these predators seek. Without information about these children, they cannot lure them into meeting them offline. Next to sexual encounters with our children, the predators seek information about our children the most.

While most of the children and teens who are lured by online sexual predators into offline meetings go willingly, the predator knowing their address, telephone number and family name, is extremely helpful in both the grooming process and in locating children who are "geographically desirable." Just as adult prefers someone who lives locally, to reduce the travel time when dating, predators prefer those closer to home as well.

And those of us in the online safety and cybercrime prevention community are waiting for the next shoe to drop: The case where offline information is used by a sexual predator to physically target a child offline. Being able to learn where they live means that the sexual predator can lie in wait on the path home from school. While the methods used by typical Internet-related sexual molestation differ from those used traditionally by offline sexual molesters and rapists, with universal access those lines are expected to blur. A few years ago, a violent child rapist used the Internet to find a map and layout of a boys private school dormitory. He used the plans he obtained to break in and rape the young students in their dorms. How long before violent sexual molesters and rapists learn how to abuse the DMCA to obtain even more targeted information about a particular child? I fear, given the current learning curve, not long at all.

Little bits of information that children give away online, the name of their soccer team, or their school, or their girl scout troop number, or favorite baseball team can, when paired

---

[1] The largest survey conducted in connection with teen girls and their Internet activities was conducted jointly by our online safety group (under our former name) and Drs. Berson (husband and wife team from University of South Florida) and surveys 10,800 teen girls between the ages of 12 and 18. Most of the participants were between the ages of 13 and 16. More information about the survey can be found at http://www.ntia.doc.gov/ntiahome/ntiageneral/cipacomments/pre/aftab/surveysummary.htm. These surveys have been replicated offline in schools and the percentages range from 12 – 14% admitting to meeting Internet acquaintances in real life. Family PC Magazine, in the Spring of 2001 conducted their own smaller survey of teen boys and teen girls. They concluded that 14% of teen boys were meeting online strangers in real life and 24% of teen girls were doing so. With approximately 30 million minors online in the United States, this has serious ramifications.

with other information, lead a sexual predator to the child's door, complete with an Internet-delivered map to their door. (A revised version of the famous online story known as :Shannon" can be found at http://www.wiredkids.org/safety/tiffany.html.) That's why we are so adamant about children and teens not sharing personally identifiable information online with anyone they don't know in real life. And many children understand this and the risks involved.

Every day we hear about the latest case of a child lured into an offline meetings and raped. Or we learn that a young girl is raped and killed (Christina Long from Danbury Connecticut last May). Every year the number of cases where online sexual predators attempt to, and are successful in, luring a child into an offline sexual encounter increases exponentially. We rely on awareness of the importance of keeping personal information to yourself as our most powerful message in this war against Internet-related child molestation. That message is now frustrated.

The ability of a sexual predator to obtain that child's address, family phone number and contact information would change all that. How do we protect children from the newest powertool in the sexual predator's arsenal? How long will it take for child molesters to realize how easy it is to obtain this information? (I regret having to raise this issue, since this affidavit itself will only help them understand how to abuse the system using the DMCA.) This one broad application of the DMCA subpoena power will frustrate the work all of the online safety community has done since 1995 to teach our children and their parents how to protect their identities online. It won't matter what they voluntarily or mistakenly give away. All the information the predators need can be obtained far more easily with the assistance of the local Federal District Court.

Certainly this isn't a real risk? Common sense tells us that the sexual predators would never risk disclosing their real identities by making the application for the subpoena, especially in a courthouse. But common sense doesn't apply when Internet sexual predators are involved. Surprisingly enough, most Internet sexual predators use their real names when luring children into offline meetings. Some have been brazen enough as to brag about themselves and their notoriety, pointing the children (or FBI agents posing as a child) to articles in which they are featured. Identifying themselves to a clerk in the District Court wouldn't faze any of them. At least not if the end result is having the child's last name, address and telephone number delivered conveniently to their mailbox. It's worth the risk.

I will share a true case, to show how far these men will go. Several months ago, a mother contacted our group. Her thirteen-year-old daughter was being blackmailed and had been forced to produce child pornography for someone she had met online. Her daughter was a "good girl" who follows the rules and never gets into trouble. She was aware of the risk of sharing her personal contact information, and never would have agreed to meet someone offline. Yet, the sexual predator managed to get to her anyway. (We will call this young girl "Susan" to protect her real identity.)

Susan received a message from someone online purporting to be another young girl in trouble. When Susan offered her help, the "young girl" said that she had been sexually victimized and didn't know where to turn. Susan, being a caring person, offered to help. She advised the "young girl" to talk with her mother about the problem. And when the "young girl" said it was hard to communicate about such intimate matters in writing, and asked for Susan's telephone number, Susan offered it to her. All the knowledge about how important it is not to give our your telephone number online didn't matter when a "young girl" needed help.

The "young girl" called Susan. But sounded more like a 50-year-old man. And he had no reservations about identifying himself as one. He told Susan that he "knew where she lived" and that unless she used her webcam to do unspeakable things on camera where he could watch (and presumably record) her acts, he would come to her home and rape and kill her. If she told her mother, he threatened to rape and kill them both. He would call and threaten her repeatedly if she didn't answer his cell phone calls on the first or second ring. She was terrorized for months -- and complied with his demands for months. Finally she broke down and confided in her mother. When her mother reached out to this man, he threatened to kill her as well. We turned this case over to the FBI's Innocent Images unit and the Internet Crimes Against Children task force in her region. But this is the kind of things that happens more often than anyone would ever believe. Sexual predators will do anything they can to reach a child offline. We shouldn't be making it easier for them to do so.

Cyberstalking and Harassment

"I know where you live and I am going to kill you.", "I know what route your children take home from school…", "Interested in "doing" nine-year-old twins?", "I am watching you…and like your new blue pajamas" or "I like your new red car, but why are your lights still on in your bedroom?" Messages like these and others arrive through our cyber-911 cyberstalking help form, and in our live help channels daily.[2] The people who receive them are frightened. And few in law enforcement take them seriously. To many it seems like "sticks and stones" to but those involved it can have much more serious consequences.[3] And technology, such as Trojan horses, allow someone to send you an infected file that allows the to watch you through your webcam or listen to you in your own home using your computer's sound card, without your knowledge.[4]

---

[2] Readers Digest in April, 2000 published a special article on cyberstalking, highlighting our work under our former name. (The name of our cyberstalking help group is now WiredPatrol.org.) Their press release about the article can be found at http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=105&STORY=/www/story/03-28-2000/0001176125.

[3] In 1999 the Department of Justice did a report on cyberstalking. It also referenced our work under our former name. http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

[4] CourtTV in its 2002 Safety Challenge special dealt with Trojan horses and risks of cyberstalking using Trojan horses to record people in their own homes, secretly. You can view videoclips from that special from the link provided at http://www.aftab.com.

Cyberstalking and harassment often moves offline. To prevent that from happening, the personal offline contact information can never be made available to the stalker. If it is, he or she[5] can use the Internet itself to assist in targeting someone for an offline attack. There are several publicized cases where the cyberstalker posted the personal contact information about the victim, offering them up for sex. Postings in sex-topic chatrooms or on message boards indicating an interest in torture, bondage or group sex is not unusual. The person's name is then posted along with their telephone number and address. People have been known to show up at their door, responding to the posts. Not all of those people leave happily when they learn of the hoax.

Cyberstalkers are typically seeking revenge or retribution for some real or imagined wrong. Those who are the most persistent (and among the most dangerous) often have romantic or sexual fixations on the victim of the cyberstalking or harassment. Sometimes there may have been sexual communications or flirtatious communications online that went sour, sometimes a cyberstalker has found a photo of their victim online and imagined a relationship with the victim, or even become a cyber-groupie of a cyber-celebrity or well-known person. But these cyberstalkings often move to real life stalkings and sometimes serious offline attacks. It is essential that the ability of the cyberstalker to locate or contact the person offline is as limited as possible. Cyberstalking victims know this, and work hard to keep their offline identities and contact information private. Their hard work would be thwarted quickly if all their stalker needed to do was walk into a courthouse and fill out a form, swearing falsely that they held a valid copyright that was being infringed.

The second most dangerous motive for cyberstalking is revenge, hate or retribution. Politics and varying lifestyles are frequent topics online. People are able to share their beliefs and interests with other like-minded people online. It's one of the most valuable features of the Internet, worldwide communication and sharing of ideas. But not all people are as forgiving or understanding of others beliefs, lifestyles or diversity. White supremacists harass minority groups online, and individual members of those groups. Post- September 11th many in the United States harassed middle eastern groups, or those they thought were middle eastern groups, as well as those posting in those online groups' sites or on their message boards. There are hate groups that harass certain religious groups. The ADL has worked diligently to stop bigotry and hate online, especially against Jewish groups and individuals identified as being Jewish. Gay and lesbian groups are also often the target of cyberstalking and harassment. Survivors of breast cancer and patients with serious and terminal diseases and medical problems are frequently attacked online, as well. As Internet Mom, Robin Raskin said, "The Internet is an equal opportunity offender." What she failed to add was that many users take offence and take action to hurt the others based on that offence. And that action can be very dangerous to their victims.

---

[5] Unlike online sexual predators who are almost always men, roughly 1/3 of the cyberstalking cases involve a female stalker.

Do we want to let hateful and vindictive people know how to find their victims offline? It's bad enough that they can find them online. Offline contact information means that they face more than "words" and hurt feelings and even fear. Offline "sticks and stones" mean the possible "breaking of bones" in the children's rhyme. You *can* be hurt by that.

Political Speech

One of the beauties of the Internet is being able to take political stands, support a political position and work to promote that position, all from the comfort of your living-room or office and anonymously. One of the beauties of being an American is being able to do this without having to give up your identity. It's the basis of our First Amendment. It's what makes us different from most of the rest of the world. In an interview with Saddam Hussein, Diane Sawyer had to explain to a surprised Hussein that in the U.S. we can openly criticize the President and the government. He was amazed, and couldn't conceive of a country where such actions are permitted. And in reality, they are more than permitted, they are encouraged. Political speech is among the most protected of all forms of speech. It is something many other regimes and cultures cannot understand. It is the essence of being American.

How free would people be in expressing their political beliefs if they knew that their IP address could be used to pierce their anonymity and obtain their real identities? This would have more than a chilling effect, it would leave them out in the cold.

Online Adoption

The Internet is a wonderful place to learn about adoption and for adoptees and birth-mothers to reach out and find each other.[6] It allows them to communicate while still protecting their real identities. It allows them to protect their offline privacy while still providing information sought by the adoptee about family medical histories, or about the myriad of questions both parties have about each other. Sometimes adoptees seek the identity of their birth-parents, when the law provides for non-disclosure of this information. Sometimes birth-parents reach out to find their birth-child, when the child doesn't wish to be found. Others just taunt and torment birth-mothers and adoptees.

Law Enforcement and Online Investigations

While not a member of law enforcement myself, our Cyberlawenforcement.org division is run by volunteers who are or used to be members of law enforcement. I serve on the Home Office cybercrime task force on their law enforcement and cybercrime prevention committees. We also work very closely with law enforcement, and frequently assist in their online investigations.

Law enforcement counts on anonymity online. Larger national and international agencies have special IPs and online accounts that can't be traced back to them. But smaller and

---

[6] There are two very helpful articles dealing with adoptions and privacy online. One, written by Laura Mansnerus for the New York Times, can be found at http://query.nytimes.com/gst/abstract.html?res=F30F1FFF3A5F0C758EDDA00894D9404482. An article that explains the kinds of abuse experienced by birth-parents online, http://www.ledger-enquirer.com/mld/ledgerenquirer/news/nation/3991997.htm.

regional law enforcement agencies often do not have this kind of identity protection when the IP-address is pierced.

Law enforcement agents often sit in child pornography chatrooms and channels in connection with child pornography and child sexual exploitation sting operations. They go undercover as a child to ferret out child molesters online. These investigations take months or even longer. How long would it be before child molesters and child pornographers would learn to use the DMCA subpoena power to “check out” a new visitor or “child victim” in their channels and chatrooms? What about when law enforcement is investigating cyber-terrorism? Death threats or bomb threats? Even criminal copyright activities? It is ironic that a tool being sought by copyright holders could be used to frustrate the prosecution of criminal cases enforcing their rights.