Global Information Assurance Certification Paper

Protecting the Online Privacy of Children
George D. Vanlandingham Jr.
February 28, 2001

Introduction

It's called by many names. The 'Web', the 'Information Super-Highway', the 'Net' or simply being 'online'. Millions of people access the Internet every day to take advantage of the vast amount of information that is available at our finger tips. We go online to exchange email, and visit with friends in chat rooms. We can find out practically anything about news, sports, and stock quotes. We shop online, bank online and even have the opportunity to further our education online. Although a majority of the people who visit the internet on a daily basis have an enjoyable experience, it does not come without risk. As the world is made up of various types of people, so is the world in cyberspace. Hackers and script-kiddies have their fun with pesky viruses and destructive viral time bombs through the promise of love, wealth or a glimpse of an attractive athlete. The mere suggestion of any of these possibilities would cause many people to open an email even if they are unsure of the sender. There are also those that will not hesitate to become the digital predators. We, as adults, have become a little more in tune with the potential for compromise within the digital realm and mostly, we do a decent job of protecting ourselves. We ensure that our anti-virus software is updated regularly, and use appropriate software or hardware with our "always-on" connections. But have we stopped to think about the potential for exploitation the little ones in our homes may be exposed to. Just as the person on the street may tempt a child into a car with the promise of candy or having been sent by a parent to pick them up, they can be tempted online as they enter contests or just try to play a game. But this temptation involves information. Information about where they live, the name of the family pet or even their favorite cereal. There are also those that will take it even further by asking an unsuspecting child information about the family and even try to get a credit card number as part of a registration process for games and contests. The Children's Online Privacy Protection Act (COPPA) was designed to protect the privacy of kids under 13 while online by requiring verifiable parental consent before collecting and/or sharing their personal information. The purpose of this paper is to give an overview of COPPA and a couple of tools at our disposal to help us protect the privacy of our kids online.

The Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act was passed by Congress on October 21, 1998. The Federal Trade Commission was required to enact rules to administer this act and the final rule became effective on April 21, 2000. A copy of the final rule can be seen at: www.ftc.gov/os/1999/9910/childrensprivacy.pdf.
This act was designed to prevent the online collection of personal data from children less than 13 years of age without verifiable parental consent. A privacy policy must be in place explaining what information is kept on the child visitor and there must also be a parental notification and approval system. Even web sites that have a small kids section or sponsor a kid's event must be in compliance with COPPA. Sites that share information

or afford the opportunity for children to do so must notify the parents offline either through a telephone call or a fax. Sites that do not share information merely have to send an email to the parents. For several years before COPPA was passed, the Center for Media Education had been monitoring and analyzing online marketing directed toward children. It was their 1996 report, " Web of Deception " that first documented abusive marketing and online data collection aimed at children. This also started a Federal Trade Commission investigation of online marketing which eventually resulted in the passage of COPPA. The act applies to websites or online services that target children and to sites that have knowledge that they collect personal information from children. A child is defined as any person that is less than 13 years old. It does not apply to any nonprofit entity but does apply to any person or company that operates a website or online service for commercial purposes or to sell products or services through the website or online service.

Personal information is defined as individually identifiable information about that individual that is collected online including:

- A first and last name;
- A physical address that includes a street name and the name of the city or town;
- Any online contact information to include an email address, instant messenger identifier, or a screen name that reveals an individuals email address;
- A telephone number or a social security number;
- A persistent identifier such as a customer number held within a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information if that combination permits physical or online contacting;
- Information concerning the child or the parents of that child that the web site operator collects online from the child and combines that with another identifier described above.

So as you can begin to see, a web site operator needs to be extremely cognizant of the type of audience they attract to their site and what, if any, information is collected from visitors.

If COPPA applies, then the web site operator must:

- Post prominent links on the web site to a notice of how they collect, use and/or disclose personal information from children;
- Notify parents that they wish to collect information from their children and obtain parental consent before using, collecting and/or disclosing that information;
- Not condition a child's participation in online activities on the provision of more personal information than is reasonably necessary to participate in that activity;
- Allow parents the opportunity to review and/or have their child's information deleted from the operator's database and to further prohibit the collection of information from the child;

- Establish procedures to protect the confidentiality, security and integrity of personal information collected from children.

There are some exceptions that permit the collection of a child's email address without getting the parent's consent first:

- To respond to a one time request from a child.
- To collect a child's or parent's email address to provide notice and seek consent.
- To respond more than once to a child's request as in a subscription to a newsletter. However, parental consent is required before the second contact.
- To protect the safety of a child who is participating on the site in a chat room.
- To protect the site or respond to law enforcement, as in a site compromise or a hack.

Now imagine yourself as the operator of a web site that catered to children or offered products and services for sale that would impact on the life of a child. Think it would be time consuming…cost ya' a few bucks? Take into account a few examples below:

A Chicago-based company said it spent more than $90,000 to comply with COPPA. The cause of the huge expenditure was the increase in staffing, administration and the need for hardware and software.

One web site that catered to young teens dealt with the compliance requirements in a different manner. They decided to not allow kids 12 and under on the site as opposed to coming up with the estimated $50,000 in additional staffing and programming in order to be in compliance with COPPA. This resulted in about a five percent drop in visitors to the site.

For one community site for children the cost has been between $50,000 and $100,000…. so far.

The fees for legal services don't run cheap either. One Internet attorney charges clients a flat fee of $10,000 to audit the child privacy policies and estimates that it will cost clients between $60,000 and $100,000 annually to stay in compliance with COPPA.

One web site that caters to kids between the ages of 6 and 13 as an online destination for games, web surfing, and talking to other kids, spent over $150,000 and three months to meet the standards set forth by COPPA. The end result was a 20 percent drop in traffic.

The penalty for each violation of the Children's Online Privacy Protection Act is $11,000.

Safeguarding Our Information

Certainly there are those that feel another law is just Uncle Sam's way of having a say in our lives or trying to regulate the free space that has become the Internet. Maybe it's just

another way to generate revenue…wait for someone to not realize that a small portion of their web site attracts children. Information gets collected and BAM!, chalk up one $11,000 penalty for the violation. Granted, the Internet is not owned by anyone. There are organizations and individuals that take part in establishing the standards that make the Internet function. Guidelines are needed to deal with those that would take advantage of unsuspecting folks and to deal with the ever growing breed of cyber criminals. Think it doesn't happen? Read on.

In September 1999, two Russian émigrés jammed U.S. Internet Service Providers as part of an email spamming scam. They sent out over 50 million emails defrauding people out of more than $250,000. The cost to complete the same task via regular mail would have been $16.5 million in postage. Obviously the Internet has given birth to a new and efficient means for the less than scrupulous to take advantage of the speed and ever growing popularity of the world wide web.

In January of 2001, an online travel agency experienced a privacy problem. As the result of a machine used for internal purposes accidentally being placed into a production environment, the names and email addresses of over 40,000 people were exposed.

A university medical center was hacked by a cyber thief who was able to obtain nearly 5,000 hospital records.

Not only is our information vulnerable to theft and exploitation through normal and accepted activities on the Internet and in our everyday lives, our information can become innocently passed along as the result of a trusting response by a child. We have to keep in mind that our children are required to attend school and are therefore a pretty captive audience. In early February of 2001, two Senators introduced legislation that would require schools to get parental permission before personal information on students could be used for commercial purposes, and would also require schools to develop policy regarding in school commercial activities. The school will also have to inform the parents with respect to whom the information was given, how it will be used and how much time in class was used in the collection of the data. One example of such information gathering techniques involved a technology firm that had supplied the school with free computers and access to the Internet, monitored the children's Internet use by gender, age and zip code. In New Jersey, elementary school students filled out a 27 page marketing survey for a cable television channel. There was no indication of the extent of the information collected through the survey. Starting to worry? Relax, better news is on the way.

Software to The Rescue

There are software packages available that can help you feel better about the content your young ones are seeing on the Internet and how that can be controlled. We'll mention two that are commercially available for about forty-dollars. They operate in similar fashion, putting to use both blocking and filtering software.

Blocking software uses a 'bad site' list and blocks access to the sites that are on the list. Some of the lists can be customized by the addition or removal of a site within the list, and some software companies keep their lists secret and do not allow the adding or removing of sites to that list. Blocked site lists need to be updated regularly, the same as with any type of anti-virus software. This can be accomplished by downloading updated lists or you may have to purchase an updated list after a certain period of time. Filtering software use keywords. It blocks access to the sites that contain the keywords, either alone or in context with other keywords. This also results in the filtering out of harmless sites due to the inclusion of innocent words. Take into consideration the two words "butt" and "sex". If the software does not filter in context, a site containing the word "button" may be blocked. A new site for "sextuplets" or for "Sussex", England may be blocked as a result of the filtered word. Two of the packages available that accomplish this mission are 'Net Nanny 4' and 'CYBERsitter 2000'.

Net Nanny 4 is a stand alone software package that lets you control how your family accesses and uses the Internet. It allows you to filter harmful sites, restrict and monitor online activities and helps to keep your personal information private. Net Nanny 4 is customizable for multiple users and does not have subscription fees for updating the lists from their database. Net Nanny 4 uses both filtering and blocking and comes preloaded with a list of allowed, or 'Can Go' sites and disallowed, or 'Can't Go' sites. The user has the ability to scan the web site lists and customize them as needed. Below is a list of the categories and criteria used by Net Nanny 4 in determining which sites are added to their lists:

- **Sexually explicit:** Any data, pictures or text involving sexually explicit behavior or nudity and erotic behavior intended to cause sexual excitement.
- **Hate:** Any data, pictures or text designed to cause intolerance, violence or harm against a person or group based on race, religion or gender. This also includes intolerant jokes and 'slurs'.
- **Violence:** Any data, pictures or text that depicts, describes or educates about the use of violence to injure one-self, others or animals.
- **Crime:** Any data, pictures or text that promotes or advocates the commission of an act that makes the offender punishable by U.S. law.
- **Drugs:** Any data, pictures or text promoting or depicting the use of illegal drugs or abuse of any substance for illegal purposes. This will not include sites dealing with legal drugs that are appropriately prescribed for medical treatment.

Net Nanny also allows the user to further customize Internet use through the following functions:

- **Personal Information Protection:** This function makes it easier to prevent family information from being given out over the Internet such as names, addresses, phone numbers and credit card information.
- **Activity Log:** Allows you the ability to track the web sites, chat rooms and newsgroups visited and the information that was sent or received.
- **User Settings:** Gives you the option to create a different profile for up to twelve people by blocking or allowing sites, activating or deactivating a word and phrase

list. The day of the week and time of day may also be specified for each user with respect to allowing or denying access to the Internet.

- **System Settings:** Warning messages and violation actions can be customized or the standard message may be used, control over the use of words and phrases can be implemented and all online chat sessions can be logged and recorded.

Net Nanny 4 is compatible with Windows 95/98/NT/2000/ME, and can be used with a dial-up, DSL or cable connection to the Internet. It supports the browsers for Microsoft and Netscape but does not support the AOL browser.

CYBERsitter 2000 is another stand alone software package that is designed to guard against what is accessed on the Internet. Originally called 'PG-13' and first released in 1993, it is manufactured by a company that has been producing Internet filtering software for over ten years. CYBERsitter 2000 has many of the same functions as Net Nanny 4. It uses both blocking and filtering. Context sensitive filtering is used to determine which sites are placed on their blocked lists. The user also has the ability to block web sites, newsgroups and chat rooms selectively. It includes databases in many different categories of sites that you may want to restrict. Simply check off the categories and the updates are done automatically in the background as you 'surf the net'. Parents have the ability to add bad sites and can also override sites that are blocked. Included is the option to log violations and control access to the Internet by the day and time.

There are a couple of neat features that CYBERsitter 2000 offers:

- **Remote Control Program:** Gives parents the ability to check on a child's activities and make changes to the settings remotely from any PC running the client software.
- **Proxy Support:** Allows for a single point of control in a proxy environment that includes authentication.
- **Daily Reports:** Activity reports can be sent to a parent or an administrator by email.

CYBERsitter2000 is compatible with the same operating systems as Net Nanny 4 and can be used with the same type of Internet connection but has the added support for the AOL browser and networked connections.

Conclusion

Children these days learn fast, and there is nothing within COPPA or the rules that administer the act that deals with the potential for kids to cheat when attempting to access a particular web site. It won't take them long to figure out that if they are not old enough to access a site, they will have to wait for a parent or even worse, they will not be able to do some things on the Internet. It will take even less time for an under aged kid to figure out that a web site operator will not be able to tell if they cheat on their age and that there is no penalty for lying about their age. Remember, it is not the responsibility of the legal system to take the place of a parent in the lives of children. COPPA and the software

available are only tools to help ensure a child's privacy is protected while online. It's up to the parents to guarantee their privacy by being a part of the digital experience.

References

URL: http://www.cybersitter.com/cybinfo.htm (19 Feb. 2001)

URL: http://www.cybersitter.com/whycyb.htm (27 Feb. 2001)

URL: http://www.netnanny.com/prod_NN4_Description.asp (19 Feb. 2001)

URL: http://www.netnanny.com/prod_NN4_Filtering.asp (19 Feb. 2001)

Magid, Lawrence. "Child Safety on the Information Highway". 1998. URL: http://www.safekids.com/child_safety.htm (20 Feb. 2001)

URL: http://www.surgeongeneral.gov/sg4kids/privacy_parents.htm (20 Feb. 2001)

URL: http://www.kidsprivacy.org/ (19 Feb. 2001)

URL: http://www.kidsprivacy.org/history.html (19 Feb. 2001)

URL: http://www.cyberangels.org/parentsguide/16b.html (19 Feb. 2001)

URL: http://www.cyberangels.org/parentsguide/16c.html (19 Feb. 2001)

URL: http://www.cnn.com/2001/TECH/internet/02/09/children.privacy.reut/index.html (19 Feb. 2001)

URL: http://www.cnn.com/2000/TECH/computing/04/25/coppa.snags.idg/index.html (19 Feb. 2001)

URL: http://www.jameshuggins.com/h/bas1/coppa_cabana.htm (20 Feb. 2001)

Lehman, DeWayne. "Children's privacy law to take effect tomorrow". 20 Apr. 2000. URL: http://198.112.59.30/home/print.nsf/(frames)/000420D726?OpenDocument&~f (20 Feb. 2001)

URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2677980,00.html (19 Feb. 2001)

URL: http://www.idg.net/ec?go=1&content_source_id=13&link_id=390492 (19 Feb. 2001)

References (cont.)

Meehan, Michael. “Travelocity confirms Web site exposed user data”. 23 Jan. 2001. URL: http://www.computerworld.com/cwi/stories/0,1199,NAV47_STO56796,00.html (19 FEB. 2001)

Delio, Michelle.”Anna Worm Writer Tells All”. 13 Feb. 2001. URL: http://www.wired.com/news/technology/0,1282,41782,00.html (19 Feb. 2001)

Last Updated: September 24th, 2017

Upcoming Training

SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive