Preventing Another Julie Amero Tragedy

Nancy Willard, M.S., J.D.
Center for Safe and Responsible Use of the Internet
Web sites: http://csriu.org and http://cyberbully.org
E-mail: nwillard@csriu.org

February 2007

Many educators are aware of the tragic case of Julie Amero, a 40 year old substitute who was convicted in January 2007 of "impairing the morals of minors" for allegedly showing students online pornography. I have thoroughly researched this case, including a review of the police reports. My report on the case is available on my web site at http://csriu.org.

Essentially, all indicators are that Julie's computer had gotten "porn trapped" because of some inappropriate online activity of students. Pornographic images started to pop-up just as the students came into the room. Julie, who has limited computer exertise, had been told not to turn off the computer. She apparently did not know how to turn off the computer or monitor. So she turned the screen away from the students and tried to get the images to go away – not realizing that this was an impossible task. By their own reports, a few students were able to briefly view images, primarily mild erotica. Most of these students knew what was happening and were intentionally trying to see what was on the screen.

It is quite evident in the case of Julie Amero, that the district's technical security was woefully and sorely lacking, Amero had not been provided with appropriate instructions on use of the computer and actions to take if inappropriate materials appear on the screen, and the investigation was thoroughly mishandled.

As I have been discussing this case in online forums, I have gotten many emails from teachers stating: "It could have been me." This is an entirely accurate statement.

But it is also important to note that this could also have been any of your students. In August 2006, the Crimes Against Children Research Center issued a report that investigated the issue of youth access to online pornography.[1] The researchers surveyed 1,500 youth between the ages of 10 and 17. This study revealed that 42 percent of youth reported being exposed to online pornography in the 12 months prior to being asked. Of that group, 66 percent said this was not intentional. The accidental access reportedly occurred because of misspelled Web addresses, pop-up advertisements, or spam e-mails. More than three-quarters of the unwanted exposures (79%) happened at home. Nine (9) percent happened at school, 5% happened at friends' homes, and 5% happened in other places including libraries.

The following point must be made absolutely clear to all school administrators and police officers: There are various forms of "malware" (malicious software) or web site with "porn traps" or "mouse traps" (a web site feature which causes other pornographic sites to popup when the

[1] Wolak, J., Mitchell, K., & Finkelhor, D. (2006). Online victimization of youth: Five years later. National Center for Missing & Exploited Children Bulletin - #07-06-025. Alexandria, VA. http://www.unh.edu/ccrc/second_youth_internet_safety-publications.html.

user tries to exit and essentially take over control of the browser). Malware and porn traps are lurking on the Internet just waiting for someone to make a mistake that will result in the display of objectionable material. Mistyping URLs or accidentally clinking on unknown links can also result in unintentional access to inappropriate material.

Because of the presence of this malware, porn traps, and other ways to get to inappropriate material, there are three essential strategies that MUST be followed by schools to seek to prevent accidental access and to prepare everyone – adults and children – with the specific knowledge of what to do if they get porn trapped.

- Technical security. Computers need effective firewalls, security software to protect against all forms of malware, and a browser that limits pop-ups. Filtering software can provide some protection (while presenting other concerns). But it is likely less effective against the malware and porn traps because these devices will frequently lead to access to sites with URLs that have not yet been found by the filtering company. Obviously, peer-to-peer networking software should never be installed on any computer that a child has access to because this can be a source of pornography and malware. Younger students should only use the Internet in more protected environments – previewed sites and closely controlled explorations.

  It is critically important that everyone understands that none of these technologies will provide 100% protection!

- Education. All Internet users – all staff (including substitute teachers) and all students – must understand how to avoid accidental access and know exactly what to do if they get "porn trapped." Unfortunately, the false security that is grounded in reliance on fallible filtering software has resulted in a failure to teach these strategies. All uses must know:

  - Read, think, then click. Never click on a link unless there are good indicators that the link will go to appropriate materials. If in doubt, don't click.

  - Don't type URLs. Some porn sites use URLs that are similar to popular sites hoping that their site will be accessed when the user mistypes the URL. Rather than trying to type URLs, users should type the name of the site in a search engine and then carefully evaluate the search return to make sure they are accessing the desired site.

  - Watch out for porn spam. Don't open suspicious email messages and never click a link in an email message unless all indicators are that it is legitimate.

  - Turn off the monitor and ask for help. If inappropriate material appears on the screen, the appropriate response for any child or adult with limited computer skills is to turn off the screen (make sure the user knows exactly how to do this) and contact someone for assistance.

    More sophisticated computer users can force quit the browser by holding the Control-Alt-Delete keys, highlighting the browser name, and clicking "End task" or "Force quit" or simply shut down the computer.

    After any event such as this, someone with computer expertise must evaluate the computer and incident to determine how it occurred and take corrective measures.

- Appropriate investigation. Anyone who is accused of intentionally accessing inappropriate material deserves the presumption of innocence because accidental access is clearly highly possible. The determination of whether such access was accidental or intentional must involve a full analysis of the situation, especially what the individual was doing before the incident and how that person responded, as well as an analysis of the computer itself. The following guidelines are recommended:[2]

    - Authorize specific, qualified personnel to conduct such analysis and establish guidelines for notification of district leadership to be followed whenever such analysis is conducted.

    - Secure the computer. Image the hard drive so that the analysis is made of a copy and the original is not damaged during the investigation.

    - Examine the computer for any evidence of "unusual" software - spyware, adware, ... These programs almost always leave signature traces in the registry, list of services or the start up menu.

    - Examine logfiles of Internet traffic to determine if the pattern of access appears to be intentional or random. When evaluating the logfiles, it is usually possible to tell if someone was engaged in intentional access. For example, a Google search, using search terms associated with inappropriate material, followed by use of links on the search return is evidence that the person specifically searched for inappropriate material. The investigator can retrace the sites in the log and see if it is possible to go from one page to another by selecting links. If malware or a porn trap was involved, the sites usually appear in a random manner and do not use any links on a given page. Another indicator is the length of time between page loads. Someone intentionally looking for material will generally spend some time looking at the site, where as pop-ups will likely emerge in a more rapid manner.

If there is any possible silver lining to the tragedy of the experience suffered by Julie Amero it is this: This case has clearly raised attention to the problem of accidental access of pornographic material, the need for more attention to security measures and education, and the dangers of falsely accusing totally innocent individuals.

Nancy E. Willard has degrees in special education and law. She taught “at risk” children, practiced computer law, and was an educational technology consultant before focusing her professional attention on issues of youth risk online and effective Internet use management in schools. Nancy frequently conducts workshops for educators. She is expanding her use of Internet technologies to deliver “virtual” presentations and classes. She is the author of two books: *Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress* (Research Press) and *Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Use the Internet Safety and Responsibly* (Jossey-Bass).

[2] Thanks to Joel VerDuin, Director, Information Services, Wausau School District, WI, for his help in outlining these standards.