Child pornography on the internet 13819

Technology

James Noble

ISC 300

Child Pornography on the Internet

In this new age of Information, the Internet has made all types of information readily available. Some of this information can be very useful, some can be malicious. Child pornography, also known as Paedophilia is one of these problems. Any one person can find child pornography on the internet with just a few clicks of the mouse using any search engine. Despite webmaster's and law enforcement officials' efforts to control child pornography and shut down illegal sites, new sites are posted using several ways to mask their identity.

The Internet provides a new world for curious children. It offers entertainment, opportunities for education, information and communication. The Internet is a tool that opens a window of opportunities. As Internet use grows, so do the risks of children being exposed to inappropriate material, in particular, criminal activity by paedophiles and child pornographers.

Many children first come in contact with the Internet at a very young age. Some children become victims of child pornography through close relatives who may have abused them. Some children become involved with chat services or newsgroup threads. It is usually through these sites that they meet child pornographers. Children may be asked to send explicit pictures of themselves taken either by a digital camera or scanned from a polaroid. The pornographer will then post the pictures on their web site, sometimes hiding them through encryption, steganography or password protecting them using a javascript or applet.

Certain efforts have been made to control child pornography through legislation. In 1977 the Sexual Exploitation of Children Act was put into Legislation. (U. S. Code : Title 18, Section 2251-2253) The law prohibits the use of a minor in the making of pornography, the transport of a child across state lines, the taking of a pornographic picture of a minor, and the production and circulation of materials advertising child pornography. It also prohibits the transfer, sale, purchase, and receipt of minors when the purpose of such transfer, sale, purchase, or receipt is to

use the child or youth in the production of child pornography. The transportation, importation, shipment, and receipt of child pornography by any interstate means, including by mail or computer, is also prohibited. The Child Protection Act of 1984 (U. S. Code : Title 18, Section 2251-2255) defines anyone younger than the age of 18 as a child. Therefore, a sexually explicit photograph of anyone 17 years of age or younger is child pornography. On November 7, 1986, the U. S. Congress enacted the Child Sexual Abuse and Pornography Act (U. S. Code : Title 18, Section 2251-2256) that banned the production and use of advertisements for child pornography and included a provision for civil remedies of personal injuries suffered by a minor who is a victim. It also raised the minimum sentences for repeat offenders from imprisonment of not less than two years to imprisonment of not less than five years. On November 18, 1988, the U. S. Congress enacted the Child Protection and Obscenity Enforcement Act (U. S. Code : Title 18, Section 2251-2256) that made it unlawful to use a computer to transmit advertisements or visual depictions of child pornography and it prohibited the buying, selling, or otherwise obtaining

temporary custody or control of children for the purpose of producing child pornography. On November 29, 1990, the U. S. Congress enacted US Code : Title 18, Section 2252 making it a federal crime to possess three or more depictions of child pornography that were mailed or shipped in interstate or foreign commerce or that were produced using materials that were mailed or shipped by any means, including by computer. With the passage of the Telecommunications Act of 1996, it is a federal crime for anyone using the mail, interstate or foreign commerce, to persuade, induce, or entice any individual younger than the age of 18 to engage in any sexual act for which the person may be criminally prosecuted. The Child Pornography Prevention Act of 1996 amends the definition of child pornography to include that which actually depicts the sexual conduct of real minor children and that which appears to be a depiction of a minor engaging in sexual conduct. Computer, photographic, and photocopy technology is amazingly competent at creating and altering images that have been " morphed" to look like children even though those photographed may have actually been adults. People who alter

pornographic images to look like children can now be prosecuted under the law. Abstracts for these laws can be found at http://www4. law. cornell. edu/uscode/18/.

The current legislation in place at the federal and state level clearly defines child pornography, and the standard sentencing for offenders. It also clearly defines a minor and what activity involving a minor is illegal. What the legislation does not do is set the standards for retreival of evidence from an electronic device, namely computers. Also, the current legislation does not set standards for decrypting child pornography that is protected. One example is the use of Steganography.

Steganography uses a bitstream algorithm to hide information in the form of raw binary code within other files suitable to hold information. The most commonly used form of Steganography uses the least significant bit of a bitmap image to store virtually any type of information. Every three bytes in a bitmap file represents a pixel. Each of these bytes represents a level of red, blue or green. Since there are eight bits in a byte, there can be up to 256 different combinations of 1's and 0's in a single byte. In the

case of a bitmap, each unique combination of 1's and 0's represents a level of red, blue or green. When the colors are combined, there is the possibility of 256^3 or 4, 294, 967, 296 different colors. In order to hide information within a bitmap file, the file in which you want to hide must be copied bit for bit into the last bit of each byte in the bitmap file. This will change each pixel of the bitmap file at the most by

1 / 2, 097, 152, depending on whether the bit being copied is the same as the bit it is replacing. Since the human eye can only physically distinguish between an average of 250 different colors, a difference of 1 / 2, 097, 152 is indistinguishable. Since only one bit of the target bitmap is being used to store information, the source file can at most be 1/8 of the size of the target file. In the case of a bitmap, a high resolution picture can easily hold a lower resolution picture that may contain child pornography.

Legally, if a bitmap image is found to contain a hidden image using steganography, there is no legal procedure for extracting that evidence for a court case. The prosecution would have to somehow explain how steganography works to a jury, and to the judge, and would have to prove

in some way that the information found did in fact come from that bitmap file. Currently, evidence found in this manner is inadmissible in court because there is no legislation dealing with this type of evidence. Also, there is no standard approved software that will decode these files. There are several software programs readily available on the internet which will encode or decode information using the least significant bit algorithm. One example is called Hide and Seek. Anyone can obtain this software free of charge, making it easy for child pornographers to hide their work.

Another problem is illicit material that is stored on a remote computer. If the perpetrator of child pornography does not own the computer that the material is stored on, it would be difficult for law enforcement officials to obtain a warrant to search a third party's computer. Also, there is currently no legislation that defines what space an a machine belongs to a specific do