Child Pornography on the Internet, Federal Laws and Corporate Responsibility

By

Ram P. Prabhu

ABSTRACT

Existing Federal laws against Child Pornography on the Internet are cited and responsibilities of U.S. corporations are identified for reporting such activities on their information technology infrastructure to appropriate FBI authorities. Discussions with FBI's Cybercrime investigation laboratory staff indicates that corporations could be liable and face penalties for not reporting known incidents of Child Pornography.

Specific tools and methods are presented that can be used by corporations for identifying, gathering, storing and protecting of critical evidence to be delivered to the law authorities in prosecuting the suspects of Child Pornography. Finally, the use of digital signature technology is recommended to guaranty authenticity, integrity and non-repudiation of the digitally stored evidence.

Child Pornography on the Internet, Federal Laws and Corporate Responsibility

April 1, 2003

Author

Ram P. Prabhu

This document is submitted as a partial fulfillment for the requirement of GSEC Certification.

TABLE OF CONTENTS

List of Figures

SCOPE

A significant amount of material appears on the Internet on the definition of Cybercrime, existing Federal Laws on Cybercrime and general pornography related issues on the Internet. In this paper we do not reproduce this material. Appropriate references are made to specific URL sites if the reader is interested in getting further information.

The focus of this paper is to create awareness for U.S. based corporations about Federal Laws on Child Pornography on the Internet, provide a guideline on what corporations can do to assist the law officials to prosecute the law breakers, and procedures that need to be implemented to avoid getting prosecuted themselves.

Specifically, we will cover the following topics in order:

- Definition of Child Pornography on the Internet and Federal Law.
- Information Technology (IT) infrastructure, actions and applications that may be considered as within a corporation's control.
- How to perform due 'diligence' to seriously try and eliminate Child Pornography from IT infrastructure under the corporation's control including a list of tools and policy guidelines.
- How and whom to report any incident of Child Pornography, how to collect and protect the evidence for law authorities to perform inspection and take further actions.
- How to verify integrity and authenticity of the evidence with non repudiation.
- What co-operation should be expected from the law authorities.

INFORMATION GATHERING PROCESS

The information presented in this paper on Child Pornography definition and law is researched from the Internet web sites listed in the 'References' section. It cites specific laws as they existed on April1, 2003. Since laws may be amended over time and web sites may come and go, it is recommended that a thorough search be performed to ensure a good understanding of the current laws on the subject.

In addition to the research on the Internet we invited and listened to two speakers from the FBI Computer Crime Prevention laboratory specialized in Cybercrime investigation. This allowed us to get a first hand understanding regarding the enormity of the Child Pornography problem and what contribution is expected from the U.S. corporations to help prevent its spread on the Internet.

DEFINITION of CHILD PORNOGRAPHY and FEDERAL LAWS

The Sexual Exploitation of Children Act[1] (18 U.S.C. 2251-2253) was enacted in 1977. Over the years there have been many amendments to this Act to further clarify the definition of 'pornography' and what makes it a 'federal crime' to possess, produce or ship Child Pornographic material. These amendments further specify which methods of distribution including the use of computer are illegal and establish the minimum punishment for such a crime.

The Child Protection Act[1] of 1984 (Act 18 U.S.C. 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. In November 1990, the U.S. Congress enacted 18 U.S.C 2252 that made it a federal crime to possess and mail three or more depictions of Child Pornography. Why do they have to be three or more? Is this a baseball game that we have to have three strikes? Do they have to be actual photographs of children or can they be computer simulated images of children having explicit sex?

Fortunately, the Child Pornography Act of 1996 amended[1] the 1984 definition of Child Pornography to include computer simulated or altered images to look like children engaged in sexual conduct. The Protection of Children from Sexual Predators Act[2] of 1998 (18 U.S.C 2252) further instituted a 'zero tolerance for possession of Child Pornography'. The legislation permits prosecution of an individual possessing just **one** matter or image of Child Pornography.

In addition to the federal laws on possession and transportation of Child Pornographic material there exist laws for 'reporting' any infractions of these laws to the federal authorities.

There are many web sites on the Internet and other resources available to the reader to understand Federal Laws on Child Pornography in more detail. Hopefully we have covered the essential minimum information for the corporations to realize that unknowingly they could be liable or prosecuted for breaking federal laws for the possession or transportation of Child Pornography material over the Internet from within the IT infrastructure under their control.

In the next section we define IT infrastructure that can be considered as one within the control of a corporation. This will be followed by suggestions to implement specific policies and tools which will assist in identifying, monitoring, documenting and reporting activities related to Child Pornography material within its IT environment.

IT INFRASTRUCTURE WITHIN CORPORATION'S CONTROL

All computers including but not limited to database and application servers, databases, applications, desktop PCs, notebooks, network routers, local area network hubs and switches, firewalls, all peripheral equipment including storage, printers, modems and one or more connections to the Internet implemented within an enterprise and used by the corporations employees or visitors can be considered as the IT infrastructure under the corporation's control.

Thus corporation could be liable for the creation, storage, printing, sending and or receiving of Child Pornographic material across this IT infrastructure including through the Internet.

Remember, the Federal Law now allows prosecution for the existence of one single matter or image of Child Pornography.

VOLUME of PORNOGRAPHY on THE INTERNET

In 1999 Dr. Agnes Fournier de Saint of Interpol's Specialized Crime Unit reported[3] that the 'Internet is unleashing a frightening wave of child pornography'. In one case alone the authorities retrieved the following evidence:

- Over 1 million still images of Child Pornography (CP)
- 67 Gigabytes of CP material
- 624 CD-ROMS
- 38 computers
- 3227 floppy disks.

The volume of CP on the Internet is continuously growing. A researcher recently identified[4] 500 CP lists advertised on the Internet containing over thousands of URLs.

In February 2003 a talk on Cybercrime given by the staff from FBI's Computer Crime Prevention Laboratory indicates that more than 80 percent of their resources are currently spending their efforts on identifying and solving Cybercrime on two specific areas: Cyber Terrorism and Cyber Pornography.

One can argue from the data recently gathered by researchers on the Internet that the Child Pornography is growing more rapidly outside the United States. However, the networked mesh of connections makes it impossible to draw arbitrary demarcation points for data carried among the domestic and international users on the Internet. As far as the law is concerned a U.S. based corporation may be considered as one involved in international business if it performs a single transaction with any customer or vendor outside U.S. Hence the problem of Child Pornography and its growth on the Internet is a universal issue.

RECOMMENDATIONS to U.S. CORPORATIONS

It may appear that the problem of Child Pornography on the Internet is so big that it is either too late to control or eliminate it entirely. However, many believe that it is never too late to start if we can stop even a single child being exploited somewhere in the world.

Following are some policies, procedures and tools recommended for implementation within a corporation's IT infrastructure to identify, combat, control and eventually (hopefully) eliminate Child Pornography on the Internet.

Policies

Users of a corporation's IT infrastructure must be made aware of the Federal law on Child Pornography and should be periodically reminded of the penalties for

breaking it. Examples of penalties are termination from employment and possible prosecution by federal authorities which may result in fines and jail terms.

Corporations need to establish a policy that clearly defines their ownership of the IT infrastructure used by the employees and the etiquettes expected when using this infrastructure.

It is a known fact that modems on the corporate systems or network can allow connections to and from the Internet bypassing the Firewall. Hence a policy must exist that does not allow any modems on the corporate IT infrastructure except in special circumstances and after approval from the IT security staff.

A policy will be needed to clearly define the need for reporting to the appropriate corporate authorities of any known use of corporate IT infrastructure for storing, printing, creating or transporting Child Pornographic material and the known use of the Internet for such activities.

Defining Federal Laws on Child Pornography and implementing specific policies on the proper use of IT infrastructure may not stop some users from creating and transporting Child Pornographic material over the Internet.

Following are some hardware and software tools to identify existence of pornographic material such as explicit pictures on systems, storage or being transmitted over the network. Specific actions can then be taken to log, filter or store such material as necessary to assist in prosecuting the suspects.

Tools

Before we discuss specific tools that will help identify pornographic material on the corporate systems it should be realized that there are ways pornographic material may be down loaded and stored on systems without the knowledge of the persons responsible for those systems.

Such down loads could take place as a result of issues such as unprotected file shares, malicious hidden codes attached to e-mail and executed by unsuspected users, auto answer modems on the systems and existing vulnerabilities on operating systems and applications. The first defense to secure the perimeter of corporate network and the IT infrastructure within is to install a good firewall with proxy and filtering. There are many software and hardware products in the market for scanning and cleaning viruses, identifying and cleaning unauthorized changes in the system kernel and files etc. Please refer to www.sans.org to understand how to take care of these and other vulnerabilities and for pointers to solutions in resolving these issues.

One of the best ways to identify pornographic material coming from or going to the Internet from a corporate network is to install filtering software on the

Firewall, on a mail server and on other systems that scans all data and identifies any 'skin' exposure ('flesh tone') such as photos or pictures of humans. Software products such as e-sweeper, Mailsweeper and Smart Filter are available in the market that can be configured to scan, quarantine, drop or forward all suspected pictures attached to messages and files based on established rules. The problem with these software packages is that they will generate many false positives identifying normal pictures of people as pornographic material depending upon flesh exposed. However, an authorized IT administrator can review the 'quarantined' pictures and determine if they should be released or stored for further investigation and or for reporting to the corporate human resources. Generally proactive scanning of end users' systems without their knowledge and or agreement may not be legal. It is recommended that the systems administrator seek legal advice before performing such proactive scanning.

Although tools such as e-sweeper and Mailsweeper may help identify some percentage of pornographic material coming in or going to the Internet from a corporate network they will not help in identifying activities such as creation, storage or printing of Child Pornographic material on the corporation's IT systems. Thus, 'reporting' of known activities relating to Child Pornographic material on the corporate IT systems becomes a very important aspect of controlling its growth on the Internet.

REPORTING CHILD PORNOGRAPHY ACTIVITIES

According to an article in Computerworld[5] of October, 2002, Director Robert Mueller of FBI speaking at a National Forum on Combating e-Crime and Cyberterrorism, said that, "We probably get one-third of the [cybercrime] reports that we would like to get." He further added that by not reporting cybercrime, "You are not enabling us to do the job."

In February, 2003 a guest speaker from the FBI Computer Crime Prevention Lab in Massachusetts confirmed that more than 60 percent of Cybercrime is not reported to them. Hence it makes it difficult for them to successfully track down suspects of Child Pornography on the Internet

We further understand from this speaker that in some cases people who do not report any known activity of Child Pornography could be liable and face criminal charges.

Thus it is important that corporations create a policy on reporting 'first hand' knowledge (i.e., not a hearsay) of creation, storage, printing or transmission of Child Pornographic material and educate its employees of such policy.

Once the existence of Child Pornographic material is positively identified on the e-mail attachments or printer or system or storage then the corporation needs to preserve the evidence for further investigation by human resources and by FBI authorities as necessary.

PRESERVATION of EVIDENCE

E-Mail Attachments and ftp

Child Pornographic material that was attached to the e-mail or sent/received through ftp, quarantined and was later positively identified as such need to be stored on the original drive where possible. A copy should be made on a non erasable media such as a WORM.

WORM acronym stands for 'Write Once Read Many'. WORM drives are available in the market that can make a permanent copy of the data on a disk using lasers. Hence it is extremely difficult to overwrite data on these discs or erase them.

It is critical to clearly identify the sender or the receiver (i.e., the owner) of such e-mail attachments or files. Most e-mail directories are based on user names or 'aliases'. On the other hand most systems on the network are identified based on their ip addresses. It is well known that ip addresses can be spoofed.

Note also that if DHCP is used on your network to assign ip addresses to systems you may need to ensure at least 30 days of lease. A large corporation where I worked in the past had no enterprise wide standards on the lease duration for ip address. When we noticed child pornographic material being down loaded from a system at one of our sites it was extremely difficult if not impossible to identify the user system since the DHCP lease at this site was only 2 days. By the time we located the suspected system it had a new ip address. As a result the human resources department did not accept the evidence as the true identity of the suspect system and or the user. Also in addition to a larger lease period for ip addresses it will help to identify the MAC address of the suspected system. Since MAC address does not change it can be a better evidence of system ownership rather than the ip address.

To monitor the activity on the suspect system it is recommended that a fix ip address be assigned to it immediately or the lease on its existing ip address should be extended indefinitely.

The date when the evidence was gathered, time, ip address, MAC address, lease period and the owner's name or alias must be confirmed without any doubt and should be so recorded with a witness such as Human Resources Manager signing for authenticity.

All drives, printouts, CDs etc. should be kept in a tamper proof enclosure for safe keeping with human resources until delivered or presented to FBI authorities.

Material Stored on the Drives. Floppies or Discs

When the existence of Child Pornographic material on data center system's or user's drives (or disks or floppies) is reported by an employee these storage media should be removed after confirming existence of Child Pornographic material and a copy should be made as a back-up. The removed media should be kept in a tamper proof enclosure until delivered to FBI authorities. Again it is extremely critical to identify the owner of the Child Pornographic material without any doubt and at least two people should sign to confirm the identity of the owner. It is recommended that the investigators document in detail the procedures they followed to identify the owner of the Child Pornographic material. In fact, it would help if the corporation can establish some standard and acceptable procedures for identifying such ownership or seek assistance from experts in this area.

Printed Material

It is extremely difficult to identify the person responsible for printing pictures of Child Pornography unless another person(s) actually witnesses the action of the suspected user and the printed copies are found in the user's possession.

Printer logs should be kept and reviewed periodically particularly after an incident of printing Child Pornographic material is reported. Again, remember that most printers keep a log of print job records based on system's ip address or user alias. These could be spoofed. Hence the owner of the printed material must be determined without any doubt. It is recommended that the investigators document in detail the procedures they followed to identify the owner of the printed material.

Maintaining Authenticity and Integrity of Evidence

Past court cases[6,12] indicate that 'Authenticity' of the material on the stored media can not be questioned by the defense unless they can provide a proof of 'evidence tampering'. However, it will significantly help the corporation in prosecuting the suspects if the corporate HR Manager (or someone representing the corporation) signs the original and a copy of the evidence as being authentic prior to storing the original in a tamperproof material.

The original evidence in digital form and a file of its 'signed hash[7] value' [Refer to Figure 1] with HR Manager's Digital Signature[8,10] should provided to the law authorities along with an agreement on specific algorithms to be used for hashing, digital signature generation and digital signature verification (The law authorities may dictate which algorithms to be used). The copy of the evidence should be retained by the corporation in a secured and locked cabinet.

As shown in Figure 1 the evidence is first hashed[7] using a hashing algorithm. The HR Manager then applies his private key to this hash value and generates a 'signed hash value' through a digital signature generation algorithm[8,10].

Exactly same procedure as above is followed to create a 'signed hash value' for the copy of the evidence retained by the corporation.

During the investigation process or court proceedings if the authenticity and integrity of the evidence are questioned then it is recommended that a new 'signed hash value' of the evidence used is calculated using the same algorithms as before with the HR Manager personally entering his Private Key (so that his private key is not revealed). The original signed hash value provided by the corporation to the law authorities should be then compared with the newly calculated signed hash value for a match as shown in Figure 2. Since mathematically it is practically impossible (or has extremely low probability) for two distinct files to yield the same hash value the authenticity and integrity of the evidence can be guaranteed if the two values match.

Non Repudiation of Signature

To ensure no repudiation by the HR Manager for signing the evidence his digital signature can be validated[8] or otherwise by using his public key as follows:

Obtain the public key of the HR Manager from the publicly available directory[9]. Create a hash value (not signed) of the evidence provided to the law authorities using the same hashing algorithm as before. Apply the HR Manager's public key to this hash value and the original signed hash value through a Signature Verification Algorithm as shown in Figure 3. The result will confirm or otherwise the validity of the signature.

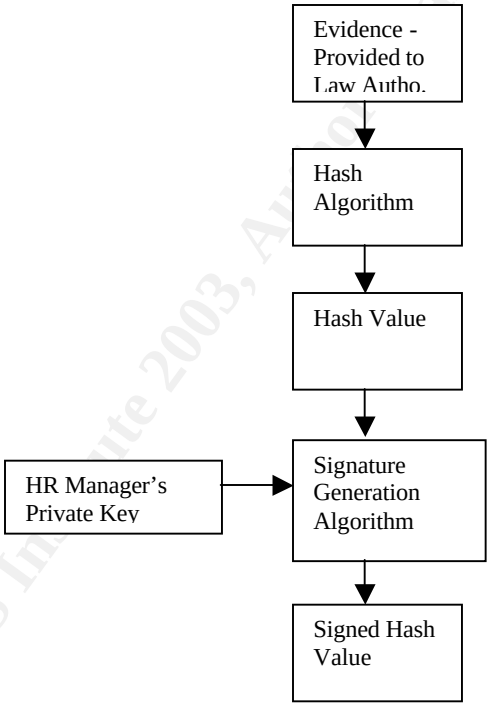

Figure 1: Creating Signed Hashed Value of the Evidence

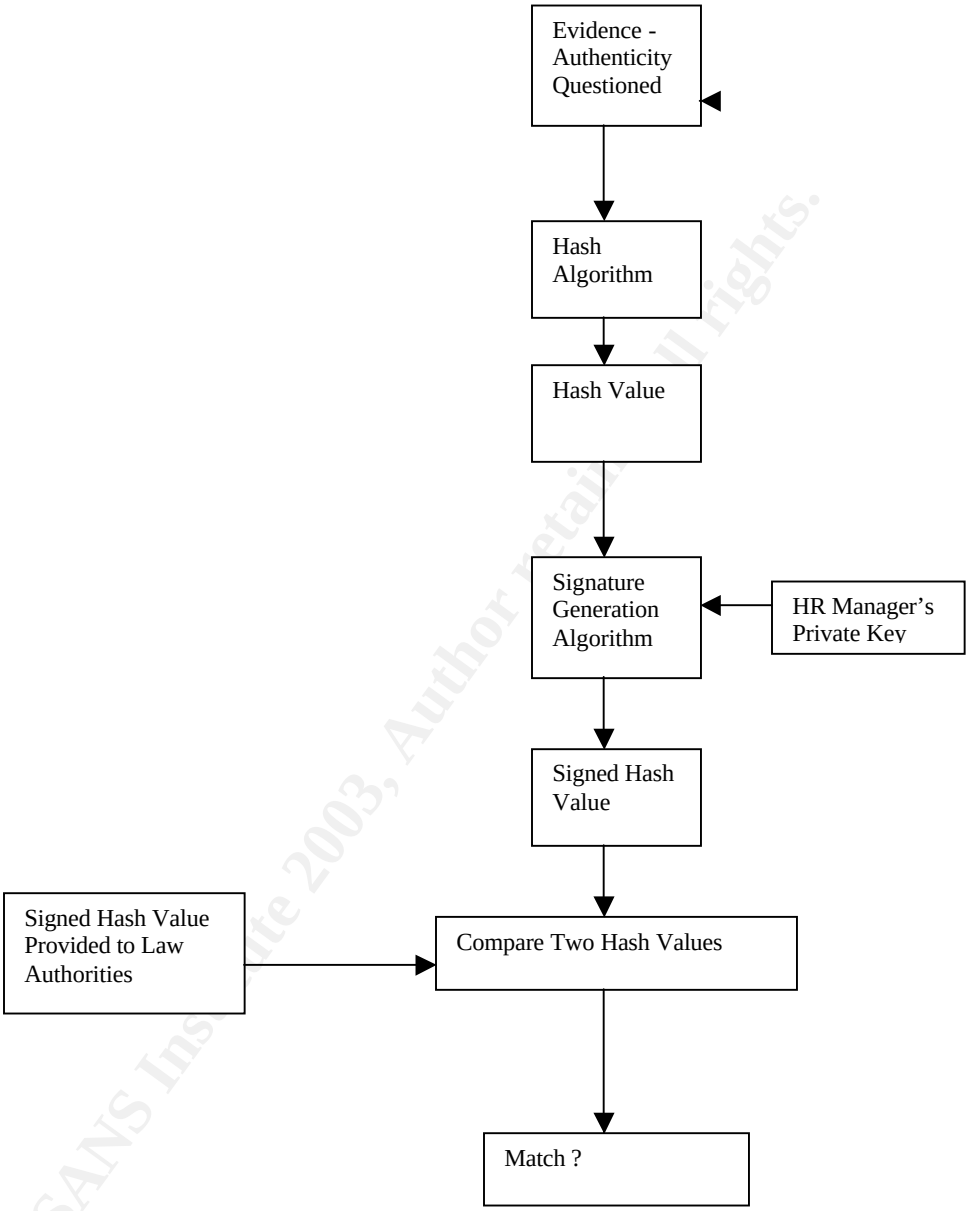

Figure 2: Validating Evidence Integrity and Authenticity

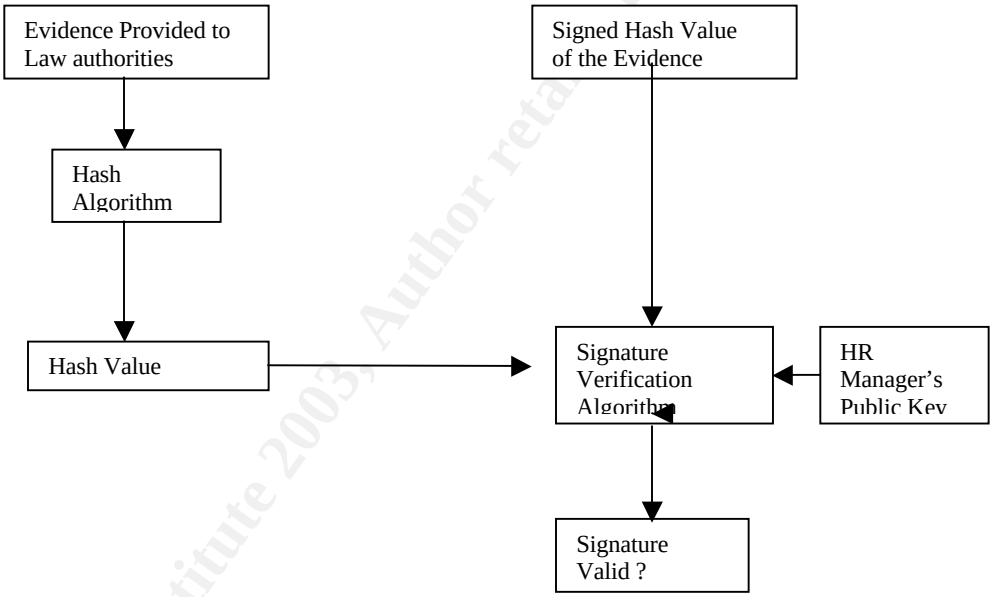

Figure 3: Signature Validation for Non-Repudiation

REPORTING GUIDELINES

As discussed earlier FBI authorities need corporations to report any Cybercrime to them immediately, specifically Terrorism and Child Pornography on the Internet. Cybercrime investigation like most other forensic investigation is very successful in identifying the suspect(s) when the evidence is not tampered with and is fresh.

After identifying the presence of Child Pornographic material within the IT infrastructure under a corporation's control it is recommended that you take the following steps immediately:

- Collect the evidence by removing hard drives, CDs, floppies, and printed matter etc.
- Make back-up copies.
- At least two responsible staff members should sign the physical media (both original and copies) such as tapes, drives and floppies containing the evidence to ensure authenticity.
- Use Digital Signature methodology to guaranty evidence authenticity, integrity and non repudiation.
- If necessary seek outside expertise in Cybercrime forensic to identify owner of the Child Pornographic material.
- Store the evidence in tamperproof containers.
- **Report** the incident to www.cio.gov and to www.ifccfbi.gov immediately.
- Assist FBI as necessary.

FBI SUPPORT

Since September 11, 2001 fight against Cybercrime is FBI's number 3 priority behind counterterrorism and counterintelligence[5]. Fighting against Child Pornography and Identity Theft on the Internet are the two top priority issues for FBI agents today. Hence corporations can expect an immediate assistance from FBI when they report incidents of Child Pornography on their IT infrastructure.

SUMMARY and CONCLUSION

Child Pornography on the Internet is exploding. FBI Cybercrime prevention and prosecution office needs assistance from corporations by immediately reporting to them any incidence of Child Pornography on the Internet that involves IT infrastructure within a corporation's control.

Persons not reporting known incident of Child Pornography on their network to or from the Internet may be legally liable.

Collecting the evidence and storing it in a tamperproof container is critical as well as maintaining its authenticity.

E-mail and file scanning tools that identify pictures with exposed skin (flesh tone) will need to be implemented on the firewall, mail servers and other systems as necessary for proactive identification of pornographic material on the corporate owned systems.

Digital signature methodology should be used to ensure authenticity, integrity and non repudiation of the evidence.

REFERENCES

1. Laws and Legislation, www.missingkids.com/html/ncmec_default_ec_chldporn_laws.html

2. Anti-Child Porn Organization, www.antichildporn.org/fedstat-cac.htm

3. Anti-Child Porn Organization, www.antichildporn.org/whiteppr.htm

4. PPSEAWA International Bulletin, Cleaning up the Net: Child Pornography, www.ppseawa.org/Bulletin/99Aug/pornography.html

5. FBI Chief: 'Lack of incident reporting slows cybercrime fight', October 2002, www.computerworld.com/governmenttopics/government/story/0,10801,75532,00.html

6. CCIPS Investigating and Prosecuting Computer Crime, www.cybercrime.gov/fedcode.htm

7. Secure Hash Standard, www.itl.nist.gov/fipspubs/fip180-1.htm

8. Network Security: Principles and Protocol Standards, Tutorial T352, Network World+Interop, 2001, Stephen Kent, GTE Networking

9. Federal PKI Directory Concept of Operations, April 1999 http://csrc.nist.gov/pki/twg/papers/twg-99-29.pdf

10. What is Digital Signature? www.youdzone.com/signature.html

11. Digital Signature Standards (DSS) www.itl.nist.gov/fipspubs/fip186.htm

12. Computer Records and Federal Rules of Evidence, www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm

13. U.S. Department of Justice, Federal Bureau of Investigation, www.fbi.gov/pressrel/pressrel02/cyberguidelines.htm

14. www.sans.org

15. NIST Computer Security division, www.csrc.nist.gov

16. ‘Cybercrime is Rising’, April, 2002, www.cnn.com