UNIT 14 PROTECTING KIDS' PRIVACY ONLINE

Structure

14.1 INTRODUCTION

Internet has become a popular source of entertainment today. It offers minors tremendous opportunities to:

- Explore new ideas
- Increase their knowledge base in a cost and time effective manner by acting as a surrogate teacher and guide
- Visit and explore indirectly foreign lands and customs and
- Offers minors opportunities to participate in challenging mental games.

Many minors, (the most recent survey on this issue revealed that in fact 90% of school children) are skilled navigators of the Internet. They are comfortable using computers and are irresistibly drawn towards the information and images that can be explored at the click of a mouse. However, certain aspects of the virtual world can be dangerous and harmful to minors. This unit endeavours to analyse the increasing trend of online crime against minors and the legislative response towards it by certain countries.

14.2 OBJECTIVES

After studying this unit you should be able to:

- enlist types and related characteristics of Internet crimes against miners;
- explore the legislative responses put into place by a set of representative countries i.e. U.S., U.K., and India;
- know some of the judicial precedents on the related issues; and
- describe some of the measures which can be implemented for shielding the minors from these heinous crimes.

14.3 INTERNET CRIMES AGAINST MINORS

Increasingly, law enforcement agencies and service providers are facing the challenge of saving child victims from Internet crimes, and in the process, considering the best way to respond to their needs and those of their families. According to cyber statistics revealed at the Federation of American scientists, there are 75 million minors and teenagers online today.

14.3.1 Types of Cyber Crime

Minors/teenagers are contacted through the Internet by criminals who:

- Produce, manufacture, and distribute child pornography.
- Expose them to child pornography and encourage them to exchange pornography.
- Entice them for the purpose of online sexual acts.
- Exploit them for sexual tourism for commercial gain and or personal gratification.

14.3.2 Characteristics of Cyber Crime

- Physical contact between the child and the perpetrator is not required.
- Repeated, long-term exposure may occur without the minor's knowledge, such as in the case when a minor's sexually explicit photograph is displayed on the Internet indefinitely.
- Minors who are victims of Internet crimes do not disclose out of fear and shame.
- Minors may not realise that they have been victimized due to lack of knowledge.
- Harassment including threats or other offensive content.
- Aggressive sexual solicitation involving offline contact.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

What are some of the types of crime that can be committed against minors?

.....

.....

.....

.....

.....

.....

14.4 LEGISLATIVE RESPONSE BY DIFFERENT COUNTRIES

14.4.1 Position in the U.S.

There are basically three primary U.S. legislations, which specifically deal with kids protection online. The Communications Decency Act (hereinafter the "CDA"), which was enacted as part of the Telecommunication Act of 1996, was the first attempt to make Internet safe for minors. The U.S. Congress made two renewed attempts to regulate minors' exposure to Internet indecency since the US Supreme Court overturned the CDA. A court injunction blocked enforcement of the first, which was the Children's Online Protection Act (hereinafter the "COPA"), immediately after its notification in 1998. However, the second legislation, Children's Internet Protection Act (hereinafter the "CIPA") was held constitutional by the Supreme Court in 2004.

(a) ***Communications Decency Act***

The CDA sought to protect minors from harmful material online by criminalizing Internet transmission of indecent materials to minors. Title V Section 203 declared that operators of Internet services were not to be construed as publishers and thus legally liable for the words of third parties who use their services. However it was struck down by the U.S. Supreme Court in *Reno* v. *American Civil Liberties Union*[1], stating that the portion intended to protect minors from indecent speech is too broad and is an unconstitutional abridgement of the first amendment and right to free speech.

(b) ***Children's Online Protection Act***

COPA was enacted to protect minors from exposure to sexually explicit materials on the Internet, 47 U.S.C. 231, which among other things, imposes a $ 50,000 fine and 6 months in prison "for the knowing posting, for commercial purposes", of world wide web content that is harmful to minors.

COPA requires that web sites and online services directed to minors under age 13 must:

- Post a clearly written privacy policy with links to the notice provided on the home page and at each area where the site or online service collects personal information from minors.
- Explain how the web site operator uses the personal information (marketing to the child? Notifying contest members?) and whether it is disclosed to third parties.

- Obtain parental consent before collecting, using or disclosing personal information about a child.
- Provide parents with the ability to review, correct, and delete information about their children collected by such services.
- Maintain reasonable procedures "to protect the confidentiality, security, and integrity of personal information collected from minors".

However, on 29 June 2004, COPA was struck down by the US Supreme Court in *Aschcroft* v. *American Civil Liberties Union*[2] on the ground that COPA was not the least restrictive means available for the government to serve the interest of preventing minors from using the Internet to gain access to harmful materials.

Another criticism which can be levied on COPA is that it does not protect the privacy of teenagers who are also minors since it is clearly applicable to minors under the age of 13.

(c) ***Children's Internet Protection Act***

The US Congress then passed the CIPA in 2000, which required the schools and libraries to install filters on computers used by minors and adults or lose federal funds.

Under CIPA, no school or library may receive discounts on Internet connectivity unless it certified that it has taken adequate steps of Internet safety. To receive the discounts, libraries must use filtering or blocking technology to shield minors from "inappropriate material on the Internet" and prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors.

However, CIPA allows the filtering technology to be disabled to "enable access for bona fide research or other purposes", including a request by an adult. To be compliant with the law, libraries must certify that they have filtering technology in place as well as a procedure to remove the filter/blocking mechanism.

(d) ***CAN-SPAM Act***

The CAN-SPAM Act which became effective from January 2004 was enacted to also address issues arising from sexually explicit e-mails. This Act requires that any e-mail messages containing sexually explicit materials must declare the contents in the subject matter itself of such e-mails. E-mails found to be in violation of this requirement can be subject to civil penalties upto USD 500,000 and also criminal consequences leading to imprisonment upto five years. Apart from labeling the sexually explicit e-mails, an option for not receiving any more e-mails with a legitimate and actual address of the sender of such e-mails has to be set out on the opening page of such e-mails. This CAN-SPAM Act would also seem to be a step in the direction of trying to address the issue of unsolicited emails to minors which contain undesirable sexual content.

14.4.2 Position in the U.K.

In the U.K., there is no specific Act, which specifically addresses the issue of online protection of minors from Internet crimes which includes but is not limited to taking, distributing, showing or publishing an indecent photograph of a child. However, certain legislations have related provisions for the such crime which can be invoked both in offline or online transgressions. These are as follows:

(a) ***Obscene Publications Acts, 1959 and 1964***

The test for 'obscenity' is set out in the Obscene Publication Acts, 1959 and 1964 respectively in section 1(1) and it is defined as material which tends to 'deprave and

corrupt' those who are likely, with regard to all relevant circumstances, to read, see or hear it.

Storage and transmission of material which is considered obscene whether for a gain or not is a criminal offence under the Obscene Publications Acts 1959 and 1964.

(b) ***Protection of Children Act, 1978***

Section 1 of Protection of Children Act, 1978 penalizes taking, making and distributing indecent pseudo-photographs of minors with imprisonment for three years or with fine not exceeding 20,000.

(c) ***Criminal Justice Act, 1988***

The Criminal Justice Act, 1988 makes it an offence for a person to have any indecent photographs of a child in his/ her possession as stated in section 160 of the aforesaid act, on top of the pre-existing offences of taking, distributing, showing or publishing such a photograph.

(d) ***Criminal Justice Public Order Act, 1994***

The Obscene Publications Acts were further elaborated and strengthened in the Criminal Justice Public Order Act, 1994 (ss.84-87) which deals specifically with 'Obscene Publication and indecent photos of minors'.

There is no specific enactment in the UK on issues related to minors protection vis-à-vis the obscene information and related problems thrown up by the Internet. However, the existing enactments have a number of provisions which can be relied upon in the event of crime related to minors on the Internet.

14.4.3 Position in India

India also does not have a legislation, which specifically provides for online protection of minors. However a related provision in the Indian Penal Code (IPC), does provide for a minor's protection from obscene material. Section 293 of the IPC penalizes whosoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of 20 years any obscene object, with imprisonment for three years or with a fine of Rs.5000.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 6 Min.*

(a) What are the legislations which are applicable to crime against minors in the US?

.....

.....

.....

.....

(b) What are the legislations which are applicable to crime against minors in the UK?

.....

.....

.....

.....

(c) What is the legal protection available for crime against minors in India?

.....

.....

.....

.....

14.5 JUDICIAL PRECEDENTS

There are very few judicial precedents on this issue of online crime affecting minors. However in the U.S. there have been a cross sections of judgments which throw some light on the effectiveness of the legislative measures enacted in the U.S. against this problem.

14.5.1 U.S. v. Fabiano[3]

Defendant John Fabiano was convicted for knowingly receiving child pornography, in violation of 18 U.S.C. § 2252(a)(2). Defendant was charged in a fifteen-count indictment with transporting, receiving and possessing child pornography in violation of 18 U.S.C. §§ 2252(a)(1), (a)(2) and (a)(4)(B). A jury convicted him on two counts of knowingly receiving visual depictions of child pornography, in violation of § 2252(a)(2), and acquitted him on the remaining thirteen counts. The district court sentenced Defendant to 24-months imprisonment and three years of supervised release.

14.5.2 U.S. v. Upham[4]

In February 1997, U.S. Customs agents who were monitoring a "chat room" on the Internet, while engaged in an undercover investigation, received in Buffalo, New York a number of images depicting child pornography. Records of the Internet service provider showed that the computer from which the images had been sent was owned by Kathi Morrissey at an address in Costigan, Maine. Acting pursuant to a warrant, the agents conducted a search of Morrissey's home on March 21, 1997.

Among the items seized and taken from the house were Morrissey's computer and a number of diskettes. Using a computer utilities program and the "undelete" function, the government was able to recover from the computer's hard disk and the diskettes some 1,400 previously deleted images of minors engaged in sexually explicit conduct. These images included the relatively small number of images that the agents had received in Buffalo in February 1997 from Morrissey's computer.

As set forth in a superceding indictment, the grand jury charged Defendant with four counts of transporting in interstate commerce computer graphic images of minors engaged in sexually explicit conduct, the production of which involved the use of minors engaged in such conduct; each count related to transmissions on a different date in February 1997. (See 18 U.S.C. § 2252(a)(1)). The fifth count charged Defendant with possession, on "a date uncertain" but between about February 7, 1997, and March 21, 1997, of the 1,400 images of minors engaged in sexually explicit conduct, the production of which involved the use of minors engaged in such conduct. See 18 U.S.C. § 2252(a)(4)(B).

14.5.3 Federal Trade Commission (FTC) v. Liberty Financial[5]

Before the COPPA Rule was implemented, the FTC addressed children's privacy in a lawsuit against Liberty Financial Companies, Inc., the operator of the Young Investor Web site. The FTC alleged that the Web site falsely represented that personal information collected from children in a survey would be maintained anonymously. The FTC alleged that the Liberty Financial Companies did not maintain the information it collected via the survey anonymously and that it maintained information about the child and the family's finances in an identifiable manner.

14.5.4 Federal Trade Commission (FTC) v. Toysmart.com[6]

Following enactment of COPA, the FTC settled a case against Toysmart.com. Toysmart.com was an online toy retailer that collected family profiles, including the names and birth dates of children, which triggered application of COPA. Toysmart.com promised in its privacy statement to never share information collected from consumers with a third party. However, the company subsequently filed a motion in a bankruptcy court seeking to sell its assets, including its database of personal information.

The FTC charged that selling the database would constitute a violation of COPA because Toysmart.com collected names, e-mail addresses, and ages of children under thirteen without notifying parents or obtaining parental consent. The FTC demanded that Toysmart.com be prohibited from selling the database as a stand-alone asset, but agreed to allow its sale within one year to a "qualified buyer" that agrees to the terms of the original privacy policy.

14.5.5 Federal Trade Commission (FTC) v. Monarch Services, Inc., Girls' Life, Inc., Bigmailbox.com and Looksmart Ltd.

In April 2001, the FTC announced settlements with three Web site operators charged with violations of COPA. The FTC charged Monarch Services, Inc. and Girls' Life, Inc., operators of www.girlslife.com, Bigmailbox.com, operator of www.bigmailbox.com and Looksmart Ltd., operator of www.insidetheweb.com, with collecting personally identifiable data from children under the age of 13 without parental consent. As part of the settlements, the companies were required to pay a total of $100,000 in civil penalties, comply with COPA in connection with any future online collection of personally identifiable data from children under the age of 13 and delete all personally identifiable data collected online from children since the effective date of COPA.

14.5.6 Federal Trade Commission (FTC) v. Lisa Frank, Inc.

In October 2001, the FTC announced a settlement with Lisa Frank, Inc., maker of popular girls' toys and school supplies that the company advertised and sold at the Web site www.lisafrank.com. In its complaint, the FTC alleged that the company failed: (1) to provide notice to parents that it wished to collect information from their children (2) to obtain parental consent for the collection of their children's information and (3) to accurately disclose in its privacy policy the company's information collection, use and disclosure practices. As part of the settlement, Lisa Frank, Inc. was required to pay a civil penalty of $30,000 and is prohibited from violating the provisions of COPA.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

Give two examples of judicial precedents which were related to crime against minors in the U.S.

.....

.....

.....

.....

.....

.....

14.6 MEASURES TO PROTECT MINORS FROM INTERNET CRIMES

Law enforcement agencies and service providers are hard pressed to find effective solutions for preventing minors from becoming victims of Internet crimes. The problems range from the fact that there exists no single legislation in various jurisdictions, which specifically provides for addressing the issues arising from such Internet crimes.

Even in the US, which is a highly developed jurisdiction, legislations like COPA which protects minors from exposure to sexually explicit materials on the Internet and penalizes the use of such material for commercial purposes have been struck down.

Legislations which are enforceable like CIPA are not of much help as they only lay down certain guidelines like filtering etc for the schools and libraries and therefore do not cover Internet crimes which actually take place and need to be punishable so that prospective criminals are prevented from committing such crimes. Then, the issue of deciding on the way forward on this extremely sensitive and topical matter. Given the grave societal concerns on this matter, there are certain steps which have been taken at various levels. Some of these are elucidated hereunder.

14.6.1 Non-legislative Measures

(a) The world bodies have gathered together and tried to come up with some effective solutions which are being globally implemented by different countries who are signatories to certain conventions of these world bodies. For instance the Council of Europe has adopted the Convention on Cybercrime, which particularly deals with infringement of copyright, computer related fraud, child pornography and violations of network security. This Convention also contains a series of powerful procedures such as the search of computer networks and interception. The main objection is "to pursue a common criminal policy aimed at the protection of society against Cybercrime, especially by adopting appropriate legislation and fostering international co-operation".

(b) Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (w.e.f. December 25, 2003)

UNICEF estimates that cross-border smuggling in West and Central Africa enslaves more than 200,000 children. The children are often "sold" by unsuspecting

parents who believe their children are going to be looked after, learn a trade or be educated. Hence the aforesaid protocol on human trafficking is extremely topical specially since it lays particular emphasis on women and children who are indeed the most vulnerable to this sort of victimization.[7]

(c) Convention on the Rights of the Child (w.e.f. September 02, 1990)

The Convention on the Rights of the Child is the first legally binding international instrument to incorporate the full range of human rights — civil, cultural, economic, political and social rights. The Convention sets out these rights in 54 articles and two Optional Protocols.[8]

The relevant Optional Protocol to the Convention on the Rights of the Child is the one on the sale of children, child prostitution and child pornography which became effective from January 18, 2002.

The need of the hour is to try and extend the provisions of all the non legislative measures with the legislative frameworks of various countries and to make these safeguards the rule of the law on a global scale. This would help to guarantee the protection of the child from the sale of children, child prostitution and child pornography.[9]

14.6.2 Technological Safeguards

Further, technology which has created this monster has also thrown up certain solutions which include the following measures:

(a) The Internet service providers have adopted various safeguard mechanisms by laying down certain guidelines for the parents to protect their children from exposure to sexual materials. British Telecom, the largest Internet Service Provider whose subscribers are BT yahoo and BT Internet have blocked child porn sites.

(b) TRUSTe is another technology created for allaying privacy fears. TRUSTe is a mark of approval and confirms that an organization has privacy practices which are monitored by third party auditors. The TRUSTe online privacy guide is available for parents and teachers to address the issues and reduce the exposure of minors to unsavoury and obscene content.[10]

14.6.3 Enforcement Measures

(a) Operation Ore launched in Britain in May 2002 is on its way out. It has details of 7300 alleged British subscribers to a child porn gateway. About 1300 people engaged in online child pornography have been arrested which included teachers, care workers, social workers, soldiers, surgeons and 50 police officers. Almost 40 minors, 28 in London are now under protective care. The investigation has focused on anyone with access to minors and in positions of authority, such as the police or magistrates.

14.6.4 Self-disciplinary Measures

Apart from legislative, non-legislative, technical and enforcement steps, in this particular instance, the parents at home and the teachers in schools have an important role to play in preventing such online crime. It would be a good idea to encourage parents and teachers to give proper guidance regarding the use of the Internet to the children and apprise them of the pitfalls which might arise during such use and result in serious transgressions. Some of the probable online crimes can be explained in simplistic terms

to the children which would help and go a long way in protecting children by simply having the children self-discipline themselves while using this important information tool. Some of the do's and don'ts which can be imparted in a straightforward and easy to understand manner to the children can include the following:

(a) access only the good educational websites;

(b) do not access the bad/deceptive websites;

(c) read the fine print on the home page of each site before proceeding to the next page of that site;

(d) do not pretend to be someone else since that can create a wrong impression and result in serious consequences;

(e) do not accept any freebies on the Internet, since those can be an inducement for luring the child into a dangerous situation;

(f) do not chat/speak with strangers without asking the parents to verify the details of such people. There have been examples of 60 year old pedophiles pretending to be young children;

(g) do not misuse the Internet to threaten or mislead others since that can have a boomerang effect.

Having explored the various threats to minors which have crept in through the Internet, it is extremely important to realise that this is one of the most savage online/offline crimes since the victims are unable to defend themselves through conventional means. Further this being more in the nature of a societal problem, apart from the legislative measures an amalgam of various technological and familial safeguards also need to be relied upon for addressing this problem. Often just by some alert parenting, exposure to this kind of crime can be easily avoided.

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 4 Min.*

(a) Give examples of two technological measures to protect minors from cyber crime?

.....

.....

.....

.....

.....

(b) Give examples of four self disciplinary measures to protect minors from cyber crime.

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

14.7 SUMMARY

- Child pornography has emerged as the major crime against minor which took place through the internet.
- The children are exposed to child pornography and are enticed by the criminals for the purpose of online sexual acts.
- The primary U.S. legislations which deals with protecting kids privacy online are the Communications Decency Act, the Children's Online Protection Act, the Children's Internet Protection Act and the CAN-SPAM Act.
- In U.K., there is no specific act, which specifically addresses the issue of online protection of minors, however, there are certain legislations which address this issue. These are:
  - Obscene Publications Acts, 1959 and 1964
  - Protection of Children Act, 1978
  - Criminal Justice Act, 1988
  - Criminal Justice Public Order Act, 1994
- India also does not have a specific legislation, however, section 293 of the IPC provides for minor's protection from obscene material.
- Measures to protect minors from Internet crimes can be divided into following categories:
  - Non-legislative measures in the form of various conventions and protocols to deal with the issues.
  - Technological safeguards to be used by ISPs.
  - Enforcement measures.
  - Self-disciplinary measures.

14.8 TERMINAL QUESTIONS

1. What makes crime against minors distinct from other conventional crimes?
2. Compare the legislative positions of all three representative jurisdictions and state which is the most effective and why?
3. How can legislative measures be improved to address this problem?
4. What in your opinion is the most important non regulative measure for controlling this menace affecting minors?

14.9 ANSWERS AND HINTS

Self Assessment Questions

1. Some of the types of crime that can be committed against minors are to:
   - produce, manufacture, and distribute child pornography.
   - expose them to child pornography and encourage them to exchange pornography.
   - entice them for the purpose of online sexual acts.

- exploit them for sexual tourism for commercial gain and or personal gratification.

2. (a) The legislations applicable in the USA are:
   - Children's Internet Protection Act
   - CAN-SPAM Act

   (b) The legislations which are applicable to crime against minors in the UK are:
   - Obscene Publications Acts, 1959 and 1964
   - Protection of Children Act, 1978
   - Criminal Justice Act, 1988
   - Criminal Justice Public Order Act, 1994

   (c) No specific Act has been enacted to protect minors from such crime in the India. However, section 293 of the IPC provides for a minor's protection from obscene material.
3. Two judicial precedents are:
   - US v. Fabiano
   - US v. Upham
4. (a) Two technological measures to protect minors against crime are:
   - Safeguard mechanisms from the Internet service providers
   - TRUSTe

   (b) Four disciplinary measures to protect minors against crime are:
   (a) access only the good educational websites;
   (b) do not access the bad/deceptive websites;
   (c) read the fine print on the home page of each site before proceeding to the next page of that site; and
   (d) do not pretend to be someone else since that can create a wrong impression and result in serious consequences.

Terminal Questions

1. Refer to section 14.3 of the unit.
2. Refer to section 14.4 of the unit.

14.10 REFERENCES AND SUGGESTED READINGS

1. US Supreme Court. 26 June. 1997. 12 Apr. 2007 <http: supct.law.cornell.edusupct/html/96-511.ZS.html>.

2. US Supreme Court. 29 June. 2004. 12 Apr. 2007 <http://www.cdt.org/speech/copa/20040629copadecision.pdf>.

3. 10th Cir. 05. Mar. 1999. 12 Apr. 2007 <http://www.kscourts.org/ca10/cases/1999/03/98-1048.htm>.

4. 1st Cir. 12 Feb. 1999. 8 May. 2007 <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court =1standnavby=caseandno=981121>.

5. Federal Trade Commission (FTC) v. Liberty Financial. File No. 982-3522. FTC 6 May. 1999.

6. FTC v. Toysmart. Civ Action 00-11341-RGS (DMass).

7. 8 May. 2007 <http://www.unodc.org/unodc/en/trafficking_victim_consents.html>.

8. 8 May. 2007 <http://www.unicef.org/crc/>.

9. 9 May. 2007 <http://www.unhchr.ch/html/menu2/dopchild.htm>.

10 TRUSTe online privacy guide. 10 May. 2007 <http://www.truste.org/pdf/Parents_Teachers_Online _Privacy_Guide.pdf>.