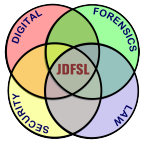

THE JOURNAL OF
DIGITAL FORENSICS,
SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 4 | Number 4 Article 1

2009

Online Child Sexual Abuse: The French Response

Mohamed Chawki
University of Aix-Marseille III

Online Child Sexual Abuse: The French Response

Mohamed Chawki, Ph.D.
Chief Judge, Egypt
Postdoctoral Fellow, ISPEC, University of Aix-Marseille III, France
Research Associate, CEDEJ (MAEE/CNRS)
chawki@cybercrime-fr.org

ABSTRACT

Online child sexual abuse is an increasingly visible problem in society today. The introduction, growth and utilization of information and telecommunication technologies (ICTs) have been accompanied by an increase in illegal activities. With respect to cyberspace the Internet is an attractive environment to sex offenders. In addition to giving them greater access to minors, extending their reach from a limited geographical area to victims all around the world, it allows criminals to alter or conceal their identities. Sexual predators, stalkers, child pornographers and child traffickers can use various concealment techniques to make it more difficult for investigators to identify them and find evidence. Others physically hide removable media and incriminating evidence in rented storage space, impeding an investigator's job to find the truth. France has given the protection of children from sexual exploitation and abuse a high priority. Traditional laws have been amended to address the challenges of information technology, violence and to bring at the same time the country into line with international conventions on the rights of children. Accordingly this current article will analyze some of the techniques used by offenders to abuse children online, including recent legal and administrative developments in France concerning online children protection.

Keywords: Cybercrime, Online child sexual abuse, Child pornography, French regulation

> ***"*** *The ability of criminals to acquire victims, gather information, lurk in cyberspace, protect or alter their identity, and communicate with other offenders makes the Internet an attractive setting for these individuals. However, at time the lack of technological sophistication displayed by offenders is surprising. Some offenders apparently are not aware that it is quite easy to locate them and make very little effort to conceal basic information on the Internet. Offenders who do not initially hide their identity may do so only after they realize they are at risk. Thus, it may be possible to use the Internet's archiving capabilities to find information on an individual before their covering behavior commenced****"***
>
> (Eoghan Casey et al., 2004)

1. INTRODUCTION

The investigation of cybercrime and the gathering of appropriate evidence for a criminal prosecution, the science of "forensic computing", "digital forensics", or "cyber forensics", can be an extremely difficult and complex issue (Walden, 2007, p. 205). This is primarily due to the intangible and often transient nature of data, especially in a networked environment. The technology renders the process of investigation and recording of data for evidence extremely vulnerable to defense claims of errors, technical malfunction, prejudicial interference or fabrication (Walden, 2007, p. 205). Such claims may lead to a ruling from the court against the admissibility of such evidence.

A lack of adequate training of law enforcement officers, prosecutors and, indeed, the judiciary, will often exacerbate these difficulties. In many countries, substantial efforts have been made over recent years to address this training need, with the establishment of specialized facilities and courses, supplemented by training courses offered by the vendors of forensic applications and services (Walden, 2007, p. 205). The true problem of the information and communications era therefore seems to be to decide exactly how much value should be attached to a given piece of information, especially when that information is stored electronically and digitally (Van der Merwe et al., 2008, p. 104).

In the past, when law enforcement investigated a crime, the investigators who analyzed the evidence used to present it to the judge to assist him in taking the correct decision. Criminal investigation training courses always include some forensics in order to understand what prosecutors and judges require in regard to evidence (Wang, 2006, p. 217). The focus is on the collection and preservation of effective evidence. In other words, at a computer-based crime scene, the highest attention must be given to specifying digital evidence. The major feature which distinguishes cyber-crime from conventional crime is that the evidence at the crime scene is represented in electronic form.[1] This also makes it easier for the criminal to store, conceal, propagate and remove the information and makes it is more difficult to identify him/her (Wang, 2006, p. 217).

In sexual offenses, the Internet may be involved in a number of ways resulting in many sources of digital evidence. It can be an instrumentality when it plays an important role in the commission of the crime, such as enticement of children to engage in sexual activity (Ferraro et al., 2005, p.4). In addition, Durkin proposes the way in which the Internet can be utilized by sex offenders to disseminate images for personal and/or commercial reasons; or to engage in inappropriate

[1] For an example on how cybercrime is complex and sometimes elusive phenomenon, see M. Chawki (2008), *Combattre la Cybercriminalité* (Perpignon, Editions de Saint – Amans) , pp. 17 – 38.

sexual communication with children and/or to locate children to abuse.[2] Lanning suggests that abusive images downloaded from the Internet may be used to desensitize and/or lower inhibitions in an offender or victim prior to or during an offense (Beech et al., 2008, p. 217). However the "stickiness" of data is attributable, in part, to the multiple copies generated by the communications process, particularly in an Internet environment, as well as the manner in which data is held and removed on electronic storage media.[3] While the "stickiness" of data will work to the advantage of an investigator, the availability of data may not enable a successful prosecution where the defendant is unaware of its existence. Conversely, the widely held perception that data held on an ICT resource is transient may work to the advantage of a defendant, where he/she can raise doubt as to the existence or otherwise of relevant forensic data.

This article takes as its theme child sexual abuse within the context of the Internet. Child sexual abuse is defined by The American Medical Association as "*the engagement of a child in sexual activities for which the child is developmentally unprepared and cannot give informed consented. Child sexual abuse is characterized by deception, force or coercion*".[4] The article sets out to provide a critical assessment of the problem of Internet child sexual abuse and its governance through French legal and non legal means. Section 2 opens by talking about the World Wide Wed and how it has increased the number of people attracted sexually to children and consequently, the increase in the number of abused minors. Section 3 is about the predominant type of On-line criminal offenses. It considers Internet sexuality and its effects on children. In this regard, four central areas of online sexuality will be discussed: cybering, online grooming, age play and exposure to online obscenity. Section 4 outlines how developments in computer technology have created new challenges to law enforcement and national governments. In this section we shall provide a brief overview of the major challenges in fight against child sexual abuse offenses on-line. Section 5 provides an analysis of the existing legislative and regulatory framework and their efficiency in combating this form of cross-border crime taking France as a case study. Section 6 discusses some measures to fight the use of Internet in illegal activities, especially with respect to child sexual abuse. Finally, section 7 is about technology evolution and how future technologies will influence the phenomenon.

---

[2] Child abusers may be classified into ***Paedophiles*** who are sexually attracted to children pre puberty, usually children younger than 11 or 12 years. ***Ephebophile*** who are attracted to adolescent boys; and ***Hebephilia*** who are offenders attacked towards both adolescent girls and boys. *See* T. Thea, *Child Sexual Abuse and the Internet*, Institut Universitaire Kurt Bosch – University of Fribourg, Report, [Feb. 2009], p. 46.

[3] For a discussion on data and digital evidence, see P.-M. Reverdy (2005), *La Matière Pénale à l'Epreuve des Nouvelles Technologies*, Thesis (University of Toulouse 1, Toulouse), p. 79.

[4] *See* T. Thea, *op. cit.* p. 15.

2. THE ROLE OF THE INTERNET IN PROMOTING CHILD SEXUAL ABUSE

> **"***The secretive, complex and sinister nature of sexual abusers who use the Internet as a means of communication and distribution of abusive images is summed up by what police found when they infiltrated the "Shadowz Brotherhood" network. Authorities say some members of the group sexually abused children and then posted the images on their Web site, which also provided advice on how to meet children in Internet chat rooms. They used sophisticated encryption techniques, sometimes hiding material in seemingly innocent picture files, officials said. Police said administrators operated a "star" system to rate members: after initial vetting, new members received a one-star rating, allowing them to view certain chat rooms, newsgroups and bulletin boards. To gain further stars they had to post images of child sex abuse on the group's site; as they gained stars, they obtained greater access to restricted sites containing the most graphic material. To further increase security, the group was structured in cells whose members knew only each other, police said***"***
>
> (The Guardian Newspaper, UK, 3rd July, 2002)

In Britain, the U.K. Cybercrime Report 2008 commissioned by online criminology firm 1871 Ltd, estimated that more than 3,543,300 offenses were committed online in 2007. There have been 830,000 instances of sex crimes – where individuals were cyber stalked or received unwanted sexual approaches by paedophiles (Garlik, 2008, p.5). The 'cyber predators' take advantage of children's attraction to the virtual world of 'Net surfing' and chat rooms (Dixon, 2002, p. 2). They use tactics and tricks to establish trust and may pretend to be another child or teenager or a sympathetic 'parent' figure (Dixon, 2002, p.2). In his article entitled "Child abuse, child pornography and the Internet" John Carr discussed whether the Internet itself has increased the number of people attracted sexually to children and consequently the increase in the number of abused children, or alternatively, if the Internet has only given us a better insight into offending behaviors that has possibly existed for a very long time.[5] He concludes that "*if we can establish that more child abuse images are in circulation and are being seen or collected by people, it is very likely the net effect is that more children are being abused now than before Internet*".[6] He presents an example from the Manchester Police"*…in 1995, arguably the last* year *before the Internet started to take off in the UK, the Greater Manchester Police Abusive Unit seized the grand total of 12 indecent images of children, all of them on paper or on Video. In 1999 the same squad seized 41,000, all bar three of which were on*

[5] *See* T. Thea, *op. cit.* p. 16.
[6] *Ibid.*

computers and had come from the Internet".[7]

The problem of sexual child abusive material can be divided into three components: the production, distribution, and downloading of images. In some cases, the same people are involved in each stage. However, some producers and/or distributors of child pornography are motivated solely by financial gain and are not themselves sexually attracted to children.

2.1 Production of Child Sexual Abusive Material

This involves the creation of pornographic images. Collectors place a premium on new child pornography material (Wortley, 2006, p. 9). However, many images circulating on the Internet may be decades old, taken from earlier magazines and films. Images may be produced professionally, and, in these cases, often document the abuse of children in third-world countries (Wortley, 2006, p. 9). Abusive images of children available on the Internet range from everyday or 'accidental' naked images of children to depictions of gross acts of indecency against a child or children, such as penetrative sexual intercourse, sadistic acts of brutality, and bestiality, with victims varying in age from babies to teenagers. (Beech et al., 2008, p. 221). Abusive images of children can also be manifested in the form of non-real or pseudo-images, including lifelike virtual abusive images without the use of actual children at all and/or those that mix different aspects and/or combinations of separate pictures to suit the user's preferences (Beech et al., 2008, p. 221). Four typical methods are used in the creation of pseudo-images: (1) an image of a child is inappropriately sexualized (e.g., clothes removed); (2) aspects of a sexualized image of an adult is given child-like qualities (e.g., reduction in breast size, removal of pubic hair); (3) an image of a child is superimposed onto a sexualized picture of an adult or child (e.g., a child holding a toy can be superimposed in a way that makes it appear that the child is holding a man's penis); or (4) a montage of abusive images can be created (Beech et al., 2008, p. 221).

2.2 Distribution and Sharing

The World Wide Web is a very attractive way of distributing information. It is also possible to set up a website that can generate revenue by selling services by subscription. The distribution of child abuse material are facilitated through commercial websites, user generated websites and peer-to-peer/file sharing network (Kierkegaard, 2008, p. 42). Offenders buy sexual pictures of minors and one can even order a live online molestation of a real child and infant for viewing. The prevalence of home video production facilitates the ease of making and posting sexual images online. Internet sex trading, where teenagers are offered goods or money in exchange for sexual favors, is on the rise (Kierkegaard, 2008, p. 42). The international policing agency Interpol's Child Abuse Image Database (ICAID) – a global database for the forensic analysis of digital images of child

[7] *Ibid.*

abuse – currently contains more than 520,000 images and has been used to identify 680 victims worldwide (Elliott et al., 2009, p. 181).

In United States v. Reedy 2000, US Postal Inspectors found the Landslide Web site advertising child pornography photos. The Texas company associated with the site, Landslide Productions, Inc., was owned and operated by Thomas and Janice Reedy. The US Department of Justice estimated that the Reedys made more than $1.4 million from subscription sales of child pornography in the one month that the Landslide operation was in business. Customers could subscribe to child pornography Web sites through a Ft. Worth post office box, or via the Internet (Casey, 2004, p. 483). Landslide also offered a classified ads section on its site, allowing Internet users to respond to personal ads for child pornography. Although related digital evidence was located in Russia and Indonesia, when investigators obtained Thomas Reedy's computer, they found more than 70 images of child pornography and a list containing the identities of thousands of Landslide customers around the world. Thomas Reedy was sentenced to life in prison, and Janice Reedy to 14 years in prison (Casey, 2004, p. 484).

On the other hand, a new market for sex work has developed online with the advent of live sex shows broadcasted via webcams (Doring, 2009, p. 1094). Some professional female sex workers have reported that their activity in cyber sex shows is much more comfortable and safe than the prostitution they previously practiced on the street or in hotels. A potential risk is faced by minors who voluntarily chose to enter into the seemingly unproblematic online sex business with excessive haste, overestimating the financial rewards while underestimating the negative psychological and social effects (Doring, 2009, p. 1094). To overcome police tracing, some Web sites use redirection to forward the customer to a completely different server, so that law enforcement must retain alert and verify which sever they are connected to when examining digital evidence.

Newsgroups provide also Internet users with a forum to discuss their sexual interests in children and to post child pornography. This service consists of several tens of thousands of themed "groups" in which any of a very large number of topics of interest is discussed offline (Sommer, 2005, p. 10). Participants do not interact in real time but "post" messages of interest to the group and to which others may comment. Participants pop into the service every now and then to see how the discussions are progressing. Offenders may use this global forum to communicate with a huge audience. They can use this global forum to exchange information, commit crimes, including defamation, harassment, stalking, and solicitation of minors (Casey, 2004, p. 485). A system of news-servers and a particular Internet protocol take care of worldwide distribution. A small number of newsgroups are devoted to paedophilia (Sommer, 2005, p. 10).

On October 16th, 1996, Sharon Rina Lopatka, an Internet entrepreneur in

Hampstead was killed in a case of apparent consensual homicide.[8] Lopatka was tortured and strangled to death by a man who met on the Internet first through Usenet and then in a BDSM channel on IRC.[9] Interestingly, nobody who knew her in person, including her husband, suspected that she was involved in this type of activity. On January 27th, 2000, the offender pleaded guilty to voluntary manslaughter, as well as six counts of second – degree sexual exploitation of a minor. He was sentenced to 36 to 53 months in prison and 21 to 26 months for possession of child pornography.[10]

In addition P2P file sharing technology provides Internet users with the potential to share local files with a potentially unlimited number of other Internet users.[11] Although one of the main drivers for the development of the technology was the sharing of music (MP3) files, as in Napster, offenders have also found the technology convenient.[12] When a file is being downloaded from a peer, the associated IP address can be viewed using netstat.[13] However, some peer – to – peer clients can be adjusted to connect through a SOCK proxy to conceal the peer's actual IP address. KazaA has one feature that can be beneficial for law enforcement. Whenever possible, it obtains files from peers in the same geographic region. Therefore, if investigators find a system with illegal materials, there is a good chance that it is nearby (Casey, 2004, p. 489).

Furthermore, live conversations between users on the Internet exist in many formats and take place 24 hours a day. One of the largest chat networks is Internet Relay Chat started in 1988 (Casey, 2004, p. 486). IRC can be accessed by anyone on the Internet using free or low-cost software. On "chat" participants have a significant degree of anonymity – they use nicknames and often adopt online personalities different from their real ones (Sommer, 2005, p. 10). Again for paedophiles an additional attraction of their specialist channels is the sense of community. Exchange of files is normally achieved by "going DCC", that is leaving the IRC server system and setting up a Direct Computer to Computer link - IRC client software usually allows users to do this by means of a simple mouse click (Sommer, 2005, p. 10).

Aside from chat networks, offenses are facilitated through online social networking sites. *MySpace* and social networking sites like it offer thriving communities where young people engage in countless hours of photo sharing.[14] In addition to *MySpace*, other social networking and blogging sites such as

[8] Available at <www.amazines.com>, [retrieved 26 October 2009].
[9] *Ibid.*
[10] *Ibid.*
[11] *See* U.S. Department of Commerce, *Peer to Peer File Sharing*, available at <www-r.gov>, [retrieved 26 October 2009].
[12] *Ibid.*
[13] *Ibid.*
[14] *See Kids Vs. Creeps: Concerns Mount Over Online Predators*, available at <www.informationweek.com>, [retrieved 26 October 2009].

Friendster.com, *Facebook.com* and *MyYearbook.com* allow users to post pictures, videos, and blogs, and they support email and instant messaging (Kierkegaard, 2008, p. 43). The two sites are different. *MySpace* is open to anyone, and has loose age restrictions. *Facebook* users are encouraged and often required to register using their real name. On *MySpace*, people talk by creating profiles: a page on the service's website which can feature a picture, blurb about oneself, a Web log (basically, an online diary), and other information. The free service also features blogs, and instant messages. Users can create their profiles and ask others to exchange materials (Kierkegaard, 2008, p. 43).

Finally, online file storage and transfer technologies may be used in sexual activities such as inappropriate file exchange with minors and in trafficking child pornography and paedophiliac text stories (Penna et al., 2005, p. 11). File transfer is performed using a variety of protocols some of which are Simple File Transfer Protocol (SFTP), File Transfer Protocol (FTP), Data Transfer Protocol (DTP), and even HTTP (Penna et al., 2005, p.11). There are three common methods for storing data online: on the users ISP server; with online file storage providers; and using a user created and provided online storage server. Anonymizing techniques may be used to provide ISPs and online storage providers with false information (Penna et al., 2005, p.12).

2.3 Consumption of Child Sexual Abusive Material

This involves accessing child pornography via the Internet. The images do not need to be saved to the computer's hard drive or to a removable disk to constitute downloading (Wortley, 2006, p. 12). In some cases a person may receive spam advertising child pornography, a pop-up link may appear in unrelated websites, or he may inadvertently go to a child pornography website (e.g., by mistyping a key word). In most cases, however, users must actively seek out pornographic websites or subscribe to a group dedicated to child pornography (Wortley, 2006, p. 12). In fact, it has been argued that genuine child pornography is relatively rare in open areas of the Internet, and, increasingly, those seeking to find images need good computer skills and inside knowledge of where to look. Most child pornography is downloaded via newsgroups and chat rooms. Access to websites and online pedophile groups may be closed and require paying a fee or using a password (Wortley, 2006, p. 12).

3. CRIMINAL OFFENSES AGAINST CHILDREN

> *Child pornography is a visual record of serious criminal offenses. Even the less extreme examples of child pornography that I saw at New Scotland Yard are records of horrifying abuse.*
>
> (Sir William Utting, 1997).

Online content and Internet activities with sexual character are widespread. The current section considers Internet sexuality and its effects on children. In this

regard, *four central areas of online sexuality* may be distinguished. These have already been established outside the Internet and have been traditionally committed in physical space. The Internet offers new configurations and possibilities of engaging children in these different areas of behavior:

3.1 Cybering

The term "cybering" has become a catchall to describe a variety of computer based sex – related behaviors (Delmonico et al., 2001, p. 4). When engaging in cybering, offenders seek to stimulate children sexually by exchanging explicit digital texts, images, and/or video – often while masturbating (Doring, 2009, p. 1095). Victims can be found in various online chat rooms, online communities, online games, or virtual worlds (e.g., Second Life). Cybering provides offenders with the opportunity to collect new sexual experiences and engage in sexual activities with a diverse range of children in a relatively safe and playful setting, behaviors contributing to sexual empowerment (Doring, 2009, p. 1095).

There are relatively few large-scale quantitative studies concerning the prevalence of cybering and even fewer national U.S.-based studies.[15] According to "Youth Internet Safety Survey" Surveys (YISS) 13 - 19% of youth have experienced some form of cybering in 2007.[16] Given the anonymity of communication, it is often difficult for youth to assess the age of solicitors, but youth reported that they believed that 43% of solicitors were under 18, 30% were between 18 and 25, 9% were over 25, and 18% were completely unknown.[17]

Studies demonstrate that violence is rare in Internet-initiated sex crimes. The evidence from the N-JOV Study (Wolak et al., 2008, p. 119) suggests that online child molesters are not among that minority of child offenders who abduct or assault victims because they have sadistic tendencies or lack the interpersonal skills to gain the confidence and acquiescence of victims (Wolak et al., 2008, p. 119). Most online child molesters are patient enough to develop relationships with victims and savvy enough to move those relationships offline (Wolak et al., 2008, p. 119). They know what to say to teens to gain their trust, arouse their sexual interest, and maintain relationships through face-to face meetings (Wolak et al., 2008, p. 119). Abduction is also rare. None of the victims in the N-JOV Study were abducted in the sense of being forced to accompany offenders (Wolak et al., 2008, p. 119). However, about one quarter of the cases started with missing persons reports because victims ran away to be with offenders or lied to parents about their whereabouts. So, in many cases, abduction may have been feared (Wolak et al., 2008, p. 119). On August, 4th 2009 an offender from Wayne

---

[15] *See* A. Schrock and D. Boyd, *Online Threats to Youth: Solicitation, Harassment, and Problematic Content*, Literature Review by the Research Advisory Board of the Internet Safety Technical Task Force, Berkman Center for Internet & Society, available at: <www.zephoria.org>, [retrieved 23 October 2009].

[16] *Ibid.*

[17] *Ibid.*

Country, Michigan was arrested on charges of cybering.[18] The suspect logged onto his laptop, exposed himself on Web cam and performed a sex act over what he though was a 13 – year – old girl but he found an undercover cyber – cop instead.[19] The offender may face up to 16 years in prison. [20]

3.2 Online Grooming

Cyber grooming is a course of conduct enacted by a suspect paedophile which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes (Marsh et al., 2009, p. 161). In the physical world, this could be venues visited by children such as schools, shopping malls or playgrounds.[21] In the process of grooming, the perpetrator creates the conditions which will allow him to abuse the children while remaining undetected by others, and the child is prepared gradually for the time when the offender first engages in sexual molestation (Childnet International, 2009). Offenders may groom children through a variety of means. For example, an offender may take a particular interest in the child and makes him or her feel his special. He may well treat the child emotionally like an adult friend, sharing intimate details about his sex life and adult relationship (Childnet International, 2009). Another grooming technique is through the gradual sexualisation of the relationship (Quayle, 2008, p. 21). Offenders thus test the child's reaction to sex by bringing up sexual matters or having sexual materials around and sexualise talking.[22] Grooming involves in essence meeting a child with the intent to commit a sexual offense; but no offense might ever be in fact committed. [23] It is conceivable that an attempted offense might be charged even where no actual meeting had taken place so the *actus reus* would simply be online conversations.[24] In the worst case scenario, the conversations might not even be with areal child but with a police investigator posing as a child.[25] The advantages of enabling police intervention as early as possible to protect the children involved are obvious, but again where should the line be drawn [26] ? Recently, Southwark Crown Court sentenced Sarah Wilson (21) for grooming a child for sex (BBC News, July 2009). The court was told that Wilson, targeted the victim in an Internet chat room and quickly began playing on the youngster's vulnerability over a six-month period, then quickly escalated into a multitude of

---

[18] Available at <www.idletechie.com>, [retrieved 23 October 2009].
[19] *Ibid.*
[20] *Ibid.*
[21] *See* Australian Institute of Criminology, Online Child Grooming Laws [April 2008], available at : <www.aic.gov.au>, [retrieved 23 October 2009].
[22] *See* P. Parkinson, *Family Law and Parent – Child Contact: Assessing the Risk of Sexual Abuse*, MULR 15, available at: <http://www.austlii.edu.au/au/journals/MULR/1999/15.html>, [retrieved 23 October 2009].
[23] Available at <www.idletechie.com>, [retrieved 23 October 2009].
[24] *Ibid.*
[25] *Ibid.*
[26] *Ibid.*

texts and phone calls becoming more and more sexually graphic (BBC News, July 2009).

3.3 Age Play

"Second life" is not even immune from sexual offenses. In everyday language, 'Second Life' is often referred to as an online computer game.[27] 'Avatars' [28] are frequently called 'players' and the conditions set up by Linden Lab [29] are considered the 'rules of the game'. (Hoeren, 2009, p. 3). The established Second Life practice of so-called ''age play'', in which users request sex with other players who dress up as child avatars has encouraged a growth in players posing as children in order to make money (Kierkegaard, 2008, p. 44). Age play is an in-world sexual activity between a child avatar and an adult avatar. Sex is an important feature in Second Life. Participants can make their avatars look like anything they want, and create software renderings of whatever equipment they want to use (Kierkegaard, 2008, p. 44). They even go to the extent of actually purchasing scripts and making the avatars engage in simulated sex. In 2009, Linden Lab created a new rating of "Adult" to encompass more extreme violent & sexual content (Second Life Website). According to these plans, any businesses located on the mainland [30] will be moved to a new collection of sims created for the purpose. Those on privately owned sims will be required to accept the Adult rating [31] or moderate their content. Residents who are not age-verified (as over-18) will not be able to access such content. The Adult rating will only apply to content or services which are advertised or publicly promoted (Second Life Website).

3.4 Exposure to Online Obscenity

Cyber pornography / obscenity, as the term suggests, is the publication or trading of sexually expressive materials within cyberspace (Wall, 2001, p. 6). The cyber porn/obscenity debate is very complex because pornography is not necessarily illegal (Wall, 2001, p.6). Child pornography may not directly physically harm

---

[27] *See* < http://secondlife.com>.

[28] An avatar is a computer user's representation of himself/herself or alter ego, whether in the form of a three – dimensional model used in computer games, a two – dimensional icon used on Internet forums and other communities. It is an "object" representing the embodiment of the user. The term can also refer to personality connected with the screen name, or handle, of an Internet user. *See* <www.wikipedia.org >, [retrieved 23 October 2009].

[29] Founder of Second Life.

[30] Premium membership allows the Resident to own land, with the first 512m² (of Main Land owned by a holder of a Premium account) free of the usual monthly Land Use Fee. Any land must be purchased from either Liden Lab or a private seller. *See* <www.wikipedia.org>, [retrieved 23 October 2009].

[31] Linden Lab has implemented a new account verification system. Users that want to access Adult regions and search results will have to authenticate their accounts by having payment information on file or by using Linden Lab's age verification system. Available at <www.pcworld.com>, [retrieved 23 October 2009].

youth each time it is viewed by an adult.[32] However, youth are harmed in the creation of images and video of illegal sexual acts, and child pornography perpetuates the idea that sexual relations with children by adults are acceptable. Those who view child pornography, for instance, may erroneously believe that the children involved are voluntary participants who enjoy the act, failing to recognize a power differential.[33]

In Europe, individuals daily consume images through the various facets of the mass media that might be called as obscene in Islamic countries. The total amount of abusive images of children available on the Internet at any one time is difficult to quantify due to the inherently dynamic nature of the system and the covert nature of the material (Beech et al., 2008, p. 218). Around 42% of U.S. youth aged 10 to 17 encountered sexualized content online in 2006 a significant increase from previous years.[34] They saw it through either wanted exposure, unwanted exposure, or both. Exact statistics on how pervasive pornographic content is on the Internet has been much-disputed but does not appear to be as pervasive as initially thought. Unwanted exposure comes from "spam" emails, mis-typing of URLs into a web browser, and key word searches that "produce unexpected results".[35]

In YISS-2, wanted exposure was indicated by 19 - 21% of minors who deliberately visited a pornographic websites.[36] Rates of exposure vary according to each country, and in some cases were reported to be higher in the U.S. In addition, increased overseas rates could be due to increased acceptance of sexualized topics, fewer technical measures such as blocking sites, and varying cultural and home environments. For instance, in a survey of 745 Dutch teens aged 13-18, 71% of males and 40% of females reported exposure to adult material in 2006.[37]

Studies demonstrate also that child molesters use both adult pornography and child pornography in the grooming process.[38] Adult pornography is most often used to arouse the victim and break down the child's barriers to sexual behavior. Child pornography is also used to break down the child's barriers to sexual behavior, but serves the additional purpose of communicating the child molester's sexual fantasies to the child.[39] Repeated exposure to both adult and child

---

[32] *See* A. Schrock and D. Boyd, *Online Threats to Youth: Solicitation, Harassment, and Problematic Content*, *op. cit.*

[33] *See* Berkman Center for Internet & Society, *Enhancing Child Safety and Online Technologies*, [December 31, 2008], p. 35.

[34] *See* A. Schrock and D. Boyd, *op. cit.*

[35] *Ibid.*

[36] *Ibid.*

[37] *Ibid.*

[38] *See* Candice Kim, *From Fantasy to Reality: The Link Between Viewing Child Pornography and Molesting Children*, Child Sexual Exploitation Update, Vol. 1, and N ° 3, 2004. Available at <www.ndaa.org>, [retrieved 24 October 2009].

[39] *Ibid.*

pornography is intended to diminish the child's inhibitions and give the impression that sex between adults and children is normal, acceptable and enjoyable. The child pornography used for this purpose depicts children who are smiling, laughing and seemingly having fun, which in turn both legitimizes sex between adults and children and portrays these sexual activities as enjoyable.[40] Of 1,400 cases of reported child molestation in Louisville, Kentucky, between 1980 and 1984, pornography was connected with every incident and child pornography was connected in a majority of cases.[41]

Table 1: Categories of Abusive Images [42]

COPINE N°	Types of Images	Description
1	Indicative	Non - erotic
2	Nudist	Naked or semi naked
3	Erotica	Photographs showing underwear
4	Posing	Deliberate posing suggesting sexual content
5	Erotic posing	Deliberate sexual or provocative poses
6	Explicit erotic posing	Emphasis on genital areas
7	Explicit sexual activity	Activity not involving an adult
8	Assault	Penetrative Sexual assault involving an adult
9	Gross assault	Penetrative assault involving adult
10	Sadistic / bestiality	Images involving pain or animal

Source: Australian Institute of Criminology

[40] *Ibid.*
[41] *Ibid.*
[42] Taylor and Quayle (2003) list ten categories of images that are used as part of the sexual repertoire of persons with a sexual interest in children. This list was developed for the Combating paedophile information networks in Europe (COPINE) centre. The COPINE taxonomy was developed principally from a psychological perspective to better understand the collecting behavior of adults with a sexual interest in children. Given this perspective, the COPINE taxonomy is more extensive than the criminal law definition. The categories are shown in this table.

Table 2: Online Sexual Offenses against Children

Offense Name	Offense Description
A) Sexual Solicitation	
- Cybering	Online communication where "the offender on the Internet tries to find a minor to talk to him / her about sex" or where the offender asks a minor to do something sexual he/she doesn't want to do, or other sexual overtures coming out of online relationships.
- Grooming	A course of conduct enacted by a suspect paedophile which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes. In this process, the perpetrator creates the conditions which will allow him to abuse the children while remaining undetected by others, and the child is prepared gradually for the time when the offender first engages in sexual molestation.
- Age play	Generally this can involve someone pretending to be younger than he actually is, but more rarely can involve assuming an older role. Variations include incest play, in which individuals recreate and sexualize roles within a family, and Daddy's girl fetishism in which real or imagined age differences are the basis of the role-playing and the female is portrayed as the younger partner.
B) Exposure to Adult Pornography Content	Pornographic content includes sexually explicit pictures, writing, or other material whose primary purpose is to cause sexual arousal, the presentation or production of this material, lurid or sensational material. Unwanted exposure to pornographic content comes from "spam" emails, mis-typing of URLs into a web browser, and key word searches that produce unexpected results. Most studies found that males are more frequently exposed to pornographic material.
C) Exposure to Child Pornography Content	directly physically harm youth each time it is viewed by an adult. However, youth are harmed in the creation of images and video of illegal sexual acts, and child pornography perpetuates the idea that sexual relations with children by adults are acceptable. Those who view child pornography, for instance, may erroneously believe that the children involved are voluntary participants who enjoy the act, failing to recognize a power differential.

4. CHALLENGING ASPECTS OF CHILD SEXUAL ABUSE OFFENSES

> *"The fact that the camera is there changes the abusive behavior of the abuser. A certain script is followed; a script that often seems to increase the violence of the abuse. The presence of a camera enhances the powerlessness of the child in the abusive situation, diminishing the child's ability to interact or to say 'No' or 'Stop' The child is performing for an audience, is given orders to smile etc., thus increasing the child's sense of complicity…"*
>
> (Anders Nyman, London, 2001)

Combating child sexual abuse on the Internet forms special challenges and this requires special expertise. Paedophile collectors of child sexual abuse images very often possess excellent computer skills, and they will continually try to find new ways of bypassing hindrances so they can live out their obsession. The Internet facilitates the ability of offenders to communicate directly with other like minded persons as well as future victims through chat rooms, newsgroups, Internet relay channels web sites and e-mail[43]. The high volume of child pornography on the Internet and the lack of international boundaries require the cooperation and sharing of information between and among national and international police departments, government legislators, and the public and private sectors[44]. This powerful medium is proving to be one of the greatest challenges law enforcement has ever had to deal with. In the following section we shall provide a brief overview of the major challenges in fight against child sexual abuse offenses on-line.[45]

4.1 Transnational Legal Jurisdictions

Domestic legislation is clearly necessary to target child pornography offenders; however, various problems with the way that child pornography is now collected and distributed make the use of domestic regulation *by itself* unworkable.[46] It is significant that the transmission of child pornography over the internet is a borderless crime because it cuts across international boundaries. Accordingly, Parliaments must focus on effective systemic enforcement of internet content by securing the cooperation of service providers at home and abroad. [47]

The new Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse is a significant measure to address the international concern

---

[43] *See* J. Fantino, *Child Pornography On the Internet: New Challenges Require New Ideas*, The Police Chief Magazine, October 2009. Available at <http://policechiefmagazine.org>, [retrieved 23 October 2009].
[44] *Ibid.*
[45] *Ibid.*
[46] *See* S. Smyth, *Mind the Gap: A New Model for Internet Child Pornography Regulation in Canada*, University of Ottawa Law and Technology Journal, Forthcoming, (Social Science Research Network), [February 21, 2009].
[47] *Ibid.*

against abuse of children and sexual exploitation both in the physical and virtual worlds.[48] Article 18 sets out the offense of sexual abuse of a child. It distinguishes two types of sexual abuse of minors. Firstly, the fact of a person engaging in sexual activities with a child who has not reached the age as defined in domestic law. Secondly, the fact of a person engaging in sexual activities with a child, regardless of this age, where use is made of coercion, force or threats, or when this person abuses a recognized position of trust, authority or influence over the child, or where abuse is made of a particularly vulnerable situation of the child. What is sadly lacking is the failure of the Convention to define the term "sexual activities". The negotiators preferred to leave to parties the definition of the meaning and scope of this term. In some countries, a naked photograph of a child is considered pornographic, while in other states, the prosecutors must prove ''intent to commit the crime" (Kierkegaard, 2008, p. 53).

Article 20(3) allows parties to make reservations in respect of the right not to criminalise the production or possession of images which either consist entirely of simulated representations or realistic images of a child who does not exist in reality, or which involve children who have reached the legal age for sexual activities as prescribed in internal law, where the images are produced and possessed by them with their consent and solely for their own private use. These two reservations exist only in relation to production and possession of such pornographic material. In spite of this omission, Member States are given discretion to criminalise morphed images. In general the treaty is a step in the right direction. The European Union should thus encourage its Member States to ratify the new Convention.[49]

Although these States have legislated against sale, production and distribution of child pornography, harmonization is urgently needed in order to combat abuse of children. One of the main issues that need to be addressed is the definition of the legal age for sexual consent. Spain sets its age of consent at 13, the rest of the countries have an age of consent between 14 and 17, except Turkey and Malta, which have the highest age limit, set at 18. In order to avoid loopholes for criminal activities, it would be important, that Member States of the EU should have a certain minimum common standard, without this it will be difficult to implement enforcement measures across Europe.

Finally, it is necessary that serious criminal offenses such as grooming be addressed by a comprehensive approach in which the constituent elements of criminal law common to all Member States, including effective, proportionate and dissuasive sanctions, form an integral part together with the widest possible judicial cooperation. The difficulty in harmonizing the definition of grooming is due partly to the lack of common definition of an agreed age definition of

[48] France has signed this Convention on 25th October, 2007.

[49] As of 24th August 2009 the Convention was signed by 35 countries and ratified by Albania and Greece only.

childhood for the purpose of protection from sexual exploitation and abuse (Kierkegaard, 2008, p. 54). For example, in Greece a child is one below the age of 8, while in other countries, it could be the age of 18. It is important that any harmonized legislation is uniform in defining what a child is.

4.2 Evidence Identification and Tracking

The dynamic and distributed nature of cyberspace makes it difficult to find and collect all relevant digital evidence in sexual offenses. Data can be spread over cities, states or even countries. When dealing with smallest networks, it is feasible to take a snapshot of an entire network at a given instant (Casey, 2004, p. 20). Moreover, network traffic is transient and must be captured while it is in transit. Once it is captured, only copies remain and the original data are not available for comparison (Casey, 2004, p. 20). Although the amount of data lost during the collection process can still be documented, the lost evidence cannot be retrieved. Once it is captured, only copies remain and the original data are not available for comparison (Casey, 2004, p. 20). Also, open networks contain large amounts of data and sifting through them for useful information can be like looking for a needle in a haystack and can stymie an investigation.

4.3 Pornography Definitions

Another aspect of the digital evidence problem in cyber offenses arises from the fact that legal definitions about pornography differ across jurisdiction and national boundaries (Beech et al., 2008, p. 218). In many cases, definitions differ between those used in legal and academic contexts and the issue is further confused by the lack of a clear legal definition of what constitutes a child as the legal age of sexual consent in many countries varies (Beech et al., 2008, p. 218). There has also been much debate as to the appropriateness of the term “child pornography”. Many academics within the field argue that the term trivializes the material and lends credence and legitimacy to the meaning that offenders bring to the phrase, while also drawing unwarranted comparison to adult pornography and thus minimizing the material’s inherently abusive nature (Beech et al., 2008, p. 218). Tate suggests that images of an abusive nature are “not pornography in any real sense, simply the evidence of serious sexual assaults on young children (Beech et al., 2008, p. 218). However, Taylor and Quayle note that the term “child pornography” carries with it an international meaning and is readily recognizable. For example, U.S. legislature explicitly uses the term “child pornography”, the British law refers to “a child involved in pornography” and the United Nations Convention on the Rights of the Child (1990) describes the “use of children in pornographic performances and materials” (Beech et al., 2008, p. 218).

The European Commission stated that “each country may reach its own conclusion in defining the borderline between what is permissible and not permissible. Therefore, a multi – layered solution is needed in this area, though

many of the proposed levels have their own debatable problems".[50]

Accordingly Wall states that "*although many so called cybercrimes are actually traditional forms of crime that can now take place through networks on a global scale, there are some that are entirely new and which require new legal strategies to resolve them*" (Wall, 2008, p. 54).

4.4 Tactics for Evasion

A further set of problems arise where an offender is using encryption. There are several situations. In the most common, parts of the suspect's stored data are encrypted – most of the PC is "open" but there are directories, sections, files, or "containers" which hold files, which are encrypted (Sommer, 2002, p. 25). This approach is popular because it is easy to implement and there are relatively large numbers of robust software products available; the computer can be used normally and then specific actions are needed to decrypt the "secret" items (Sommer, 2002, p. 25). Moreover, some IRC clients support encryption, making it more difficult for investigators to monitor communications and recover digital evidence (Bocij, 2004, p. 120).

A good example of an organized pedophile group involves a police operation known as "Operation Cathedral", which took place in 2001 (Bocij, 2004, p. 120). This was an international investigation that began after U.S. Customs officers exposed a pedophile gang called "The Orchid Club" in 1996, and found three British citizens associated with its activities (Bocij, 2004, p. 120). The operation was responsible for uncovering the activities of a notorious pedophile ring known as" The Wonderful Club". Membership of the club was open only to "serious players" who owned personal collections of more than 10,000 images of children (Bocij, 2004, p. 120). To gain some idea of the scale of the group's activities, police discovered that more than 750 000 incident images of children were exchanged via the Internet (Bocij, 2004, p. 120). When the club members knew that they were under investigation, they did not disperse but began using more sophisticated concealment techniques such as moving to IRC servers frequently and using encryption (Bocij, 2004, p. 120). In one instance, an offender's computer was sent from Britain to the FBI to decrypt the contents but to no avail. This has lead to the low level of prosecution compared to the number of individuals involved.

Offenders can make it more difficult to locate them on IRC by using the invisibility feature (Casey, 2004, p. 497). However, this feature does not conceal the offender from other Internet users in the same channel, so this offers limited protection. One advanced aspect of IRC that some criminals use to conceal their IP address are "bots" (Casey, 2004, p. 497). These programs can work like

[50] *See* Y. Akdeniz, *The Regulation of Pornography and Child Pornography on the Internet*, Center for Criminal Justice Studies, Law Faculty, University of Leeds. Available at Social Science Research Network Website <www.ssrn.com>, [retrieved 26 October 2009].

proxies and are used to perform various tasks from administering a channel to launching denial of service attacks. "Eggdrop" is one of the more commonly used IRC bots and can be configured to use strong encryption that conceals the contents of its logs and configuration files making it necessary to examine network traffic to observe nicknames and passwords (Casey, 2004, p. 497). Finally, cyber offenders who are more technically savvy and are especially interested in concealing their identity, send messages through anonymous or pseudonymous services. When an email is sent through an anonymous remailer, identifying information is removed from the email header before sending the message to its destination (Casey, 2004, p. 499). The most effective anonymous remailers are quite sophisticated and make it very difficult to determine who sent a particular message. Some remailers keep logs of the actual email addresses of individuals, but many of them will perish than make such concessions, even when illegal activity is involved (Casey, 2004, p. 499). There is a possibility that investigators can compel a pseudonymous remailer to disclose the identity of the sender but it requires significant effort since their business is to protect the identity of their users (Casey, 2004, p. 499).

5. THE FRENCH APPROACH TO CHILD ABUSE REGULATION

If some illegal and harmful content on the Internet needs to be regulated then the question is: how should this be achieved? Legislation is probably not the whole answer, and this conclusion appears to be shared by the French government. There appears not to be a single solution for the regulation of illegal and harmful content on the Internet because, for example, and as we have seen the exact definition of offenses such as child pornography varies from one country to another and also what is considered harmful will depend upon cultural differences. Although national legislation may not be efficient to combat illegal and harmful content on the Internet, it will still be needed.

5.1 Legislative Attempts to Regulate Child Sexual Abuse

France is a signatory to all the significant treaties dealing with children rights.[51] The Civil Code defines minors as individuals of either sex who have not yet reached eighteen years of age (Article 488).[52] Law 98-468 of June 17, 1998,[53] reinforcing the prevention and punishment of sexual offenses and increasing protections for minors against sexual predators distinguishes several categories of sexual offenses according to their nature and their gravity. Provisions of this law

[51] *See* for example: Minimum Age Convention 1973; Convention on the Rights of the Child 1989; Optional Protocol to the Convention on the Rights of the Child, on the Sale of Children, Child Prostitution and Child Pornography 2000; European Convention on Human Rights 1950; Hague Convention on Jurisdiction, Applicable Law, Recognition, Enforcement and Cooperation in Respect of Parental Responsibility and Measures for the Protection of Children 1996

[52] However the age for consent to sexual intercourse is currently 15 years.

[53] Law 98-468, June 17, 1998, J.O., June 18, 1998, at 9255

concerns rape, sexual assault, indecent assault, and corruption of minors. Under Article 227-2 of the Criminal Code, encouraging or attempting to encourage the corruption of a minor is punishable by five years' imprisonment and a €75,000 fine. These penalties are raised to seven years' imprisonment and a fine of €100,000 if the minor is less than fifteen years old; or has been put in contact with the perpetrator by the a telecommunication network. In addition, several provisions of French Criminal law make the following an offense:

- The use or the incitement of an under aged person to participate in a pornographic scene including photos, tapes, recordings, etc.
- The production or the distribution of any materials containing under aged persons engaging in pornography.
- The possession of pornographic materials containing minors engaging in pornography.

The penalty for the performance of these actions is set as imprisonment for a period between two and ten years and a fine from € 30,000 to € 75,000. The penalty is subject to a number of aggravations and attenuations depending on the specific circumstances specially if the offense was committed on the Internet. A striking feature of this law, which makes it different from American laws is that it is also applied to pornographic images of persons whose facial features is of a minor, unless it is proven that the person was 18 years old on the day his or her image was taken (Article 227 – 23).[54]

The French Criminal Code makes it an offense for any person who solicits, accepts, or obtains sexual relations with a minor or who engages in prostitution in exchange for remuneration or promise of remuneration.[55] The offender will be subject to imprisonment for 3 years and a fine of €45,000. Punishment is enhanced to imprisonment for 5 years and a fine when the act is committed habitually or against more than one person , or where the victim was put in contact with the offender by the use of a telecommunication network.[56] The Code provides for extraterritorial application of the French law in cases where the above-mentioned acts were committed abroad by a French national or by a forgiener residenet on the French territory.[57] In November 2003, a French citizen on vacation in the Solomon Islands was found guilty of having sex with a minor (Agence France Press). In December 2003, another French citizen was charged with child sex offenses against two teenage boys in Cambodia (Agence France Press). In February 2004, a Cambodian court charged a French citizen with sexually abusing five minors aged 12 and 14. In August 2004, a French bar manager working in Phnom Penh was arrested on suspicion of having sex with

[54] Offense added by Law 2002 – 305, 4th March 2002.
[55] Article 225-12-1
[56] Article 225-12-2
[57] Article 225-12-3.

nine children as young as 12 years of age (Agence France Press). In January 2005, a Cambodian court sentenced a French tourist to 15 years in jail for having sex with two teenage boys (Agence France Press). On a different note article 131 – 36 – 1 of the French Penal Code submits sexual convicts to surveillance and in some cases, to mandatory medical treatment to prevent further relapses. Failure to carry out the obligations set by the court may result in an additional term of imprisonment (two years maximum in cases of *délits* and five years in the cases of *crimes*).[58]

In addition, several provisions of French Law [59] aim at improving the reparation of moral and physical damages caused to victims of sexual predators. Accordingly the public prosecutor may request a medical-psychological evaluation in the early stage of the investigation to better appreciate the extent of the damage inflicted on the minor and to determine the best treatment for victims.[60] The costs of treatment are fully covered by national health insurance.[61] Hazing has become a criminal offense and is punishable by six months' imprisonment and a fine of €7,500 (Article 225-16-1).

The French Criminal Code prohibits also all forms of procuring (assisting, protecting the prostitution of others; making profits out of the prostitution of others; sharing the proceeds of prostitution of others; receiving income from a person engaged in prostitution; hiring a person for prostitution; or pressuring a person to practice or continue to practice prostitution). Punishment for procuring is imprisonment for 7 years and a fine of €150,000.[62] The Code imposes the same penalty on any person who commits actions related to procuring, including acting as an intermediary between a person in prostitution and a person who exploits or compensates the prostitution of the other; assisting a procurer in proof of false financial resources; impeding the prevention efforts, control assistance, or reduction efforts of qualified agencies on behalf of persons in danger of becoming prostitutes or of engaging in prostitution; and being unable to account for an income compatible with one's lifestyle while living with a person habitually engaged in prostitution.[63]

Punishment is enhanced to imprisonment for 10 years and a fine in case of aggravated circumstances, such as when the act of procuring is committed against a minor [64] or against a person who "*because of his age, sickness, infirmity, mental*

[58] There are three grades of criminal offenses under French law: *crimes*, *délits*, and *contraventions*. *Crimes* include, for example murder, armed robbery, rape, etc. *Délits* are the largest group of offenses in France and include sexual violence, theft, fraud, and assaults among others. *Contraventions* are punishable only by a fine, they include traffic offenses.
[59] Criminal Law, Civil Law and Criminal Procedures Law.
[60] Article 706-48, Code of Criminal Procedures.
[61] Assurance Maladie.
[62] Article 225 – 5.
[63] Article 225 – 6.
[64] Article 225 – 7 -1.

or physical deficiency, or pregnancy is particularly vulnerable and whose vulnerability is apparent to the procurer".[65] Punishment is also enhanced if that offense is committed against several people [66] or against a person who was incited to engage in prostitution either outside France or upon arrival to France. According to Article 225-7-1 if the offense of procuring is committed against a minor under 15 years of age, punishment is enhanced to imprisonment for 15 years and a fine of € 3,000,000. When an organized crime group commits the procuring, the punishment is imprisonment for 20 years and a fine of €3,000,000. In 2004 the French police cracked a baby trafficking ring in Bobigny, near Paris. Investigations began when a young Bulgarian mother reported that her 2 years old baby has been kidnapped.[67] According to investigators, she had, in fact, sold him. By approaching the police, the woman hoped to take revenge on the baby traffickers, who had paid her less than promised.[68]

Early this year the French Council of Ministers examined a new law entitled "*Loi d'Orientation et de Programmation pour la Sécurité Intérieure.*[69] This law is intended to update the policy of internal security in France for the period 2009 – 2013. Article 4 foresees the blocking of internet sites that contain child pornography.[70] The Ministry of interior will transmit their blacklist of banned sites to ISP's, which have to block the access to the "Internet addresses". Investigators would also be able to see and record in real time, from a distance, the data that appears on a computer screen, even when the data are not stored. The law would allow the French government to install keylogger software that can "observe, collect, record, save, and transmit" keystrokes from computers on which it is installed. In essence, it allows for government-installed Trojans for a period of four months; the competent judge can extend this period.

5.2 Co-Regulation and Internet Service Providers

Although the status of ISPs in France is very much debatable, for instance, whether they are publishers, distributors or common carriers, the Internet industry should also have a similar responsibility. The tricky question remains: how to achieve this? While it may be difficult to control the content of the Internet, its provision by the ISPs may be controlled. In France *La Loi pour la Confiance dans l'Economie Numérique LEN* defines the liability and clarifies the role and

[65] Article 225-7-2.
[66] Article 225-7-3.
[67] Available at <www.protectionproject.org>, [retrieved 30th October, 2009].
[68] *Ibid*
[69] Domestic Security Orientation and Programming Law (LOPSI).
[70] The first European country where ISPs started to filter the internet was the UK, in 2004, some months before Norway. In the British situation however, it is not the government but the Internet Watch Foundation (IWF) that maintains a so-called blacklist. *See* Stol, W.Ph. et al. (2009), *Governmental Filtering of Websites: The Dutch Case*, Computer Law & Security Review 25, p. 252.

responsibility of ISPs. [71] The objective of this law is to provide impetus to the digital economy in France in order to reinforce confidence in the use of such new technology and thereby ensure its growth.[72] This law has transposed the E-commerce Directive 2000/31/CE into French law together with part of the Directive on Privacy and Electronic Communications 2002/58/EC. The LEN has been heavily modified during its passage through the pipeline of parliamentary procedure [73] and has been the subject of criticism and met with vociferous opposition from a number of quarters, in particular ISPs and user groups, claiming the draft LEN threatened free expression on the Internet and placed a significant and unfair burden on ISPs to censor online content (Taylor, 2004, p.270). Many actions have also been undertaken by EDRI-member IRIS which launched a petition against this provision in the draft law, together with the French Human Rights League, the G10-solidaires association of trade-unions, and two non commercial providers.[74] The petition has been signed by more than 8.000 individuals and 170 organisations.

Other actions have been undertaken by Odebi, an association of Internet users, and by Reporters without Borders (RSF).[75] Considerable lobbying continued prior to the second reading of the Bill by the Senate which took place on 8th April, 2004. At the second reading, the Senate voted to adopt the LEN, but with certain crucial modifications. Actually article 6 provides that ISPs are not liable for information transmitted or hosted unless they have actual knowledge of illegal activity or information of facts or circumstances from which the illegal activity or information is apparent; or if upon obtaining such knowledge or awareness they act expeditiously to remove or to disable access to the information. With respect to contractual provisions on ISP's liability, it should be noted that these provisions are not enforceable against third parties in France. As a result, a contractual

---

[71] Before adopting this law, the responsibility of ISPs was governed by the French law n°2000-719 of 1st August 2000. Under this law, ISPs were liable under French civil or criminal responsibility for the illegal content of the web sites to which they provide access, only if they have not promptly undertaken the appropriate measures to block access to such content after a judicial decision. *See Estelle Halliday v Valentin Lacambre* (Paris Court of Appeal, 10th February 1999).

[72] « *Elle a pour objectif d'adapter la législation actuelle au développement de l'économie numérique afin de renforcer la confiance dans l'économie électronique et d'assurer le développement de ce secteur, tout en établissant un cadre juridique stable pour les différents acteurs de la société de l'information* ». Sénat (2007), Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, Report, Paris. Available at <www.senat.fr>, [retrieved 26th October, 2009].

[73] In fact the Senate has deleted the amendments to Article 2 of the LEN covering the regime governing the responsibility of ISPs that had been included by the National Assembly. This thereby removed the specific obligation to monitor certain types of content including paedophile and racist material, which undermined the general principle of no obligation to monitor content generally, *See* D. Taylor *op. cit.* p. 270.

[74] *See* French Draft Law Obliges Providers to Monitor Internet, available at <www.edri.org>, [retrieved 26 October 2009].

[75] *Ibid.*

exemption of liability cannot be used with regard to a third part (not subscribing with an ISP) who has suffered harm as a result of unlawful content broadcast on the networks, for example or an act of infringement. person habitually engaged in prostitution.[76]

On a different note *The Association des Fournisseurs d'Accès et des Services Internet* (AFA) [77] requires its members to offer their customers tools for (i) the filtering of illegal or harmful content; (ii) the regulation of unwanted bulk mail; (iii) a point of contact for the reporting of illegal or harmful content. In this way the responsibility for receiving or sending content is passed back to the customers – the customers are given the tools to determine themselves what information (illegal, harmful, necessary etc) they would like to receive or send.[78] The AFA makes a specific reference to the workings of the Internet Content Rating Association (ICRA) in offering systems capable of filtering content (both against illegal and harmful content and for the protection of minors) and members are expected to abide with ICRA's procedures. The implication of the rules relating to illegal and harmful content is: [79]

- An ISP has no responsibility to monitor and remove material on its own initiative;
- If the ISP removes information at the request of law enforcement agencies or private organisations acting as monitors of Internet content it should not be held responsible for the removal;
- If on the other hand an ISP does not follow the requests of law enforcement agencies and private organisations then it is in breach of these rules and may be liable for the consequences.

AFA does not have a formal complaints mechanism. When complaints are received they are passed onto the member and it is up to the member to handle the complaint.[80] The Statute founding AFA as an association, however, allows for a member to be expelled from the association, amongst other reasons, if the member acts against rules set by the AFA. In both cases member ISPs apparently follow the rules of their association.[81] It can be argued that in certain

[76] Article 225 – 6.
[77] The AFA was created in 2000; it is the amalgamation of two previous associations: the Association Française des Professionnels de l'Internet created in 1996 and the Association des Fournisseurs d'Accès à des Services en ligne et à l'Internet created in 1997. Both associations were set up mainly to define common practices regarding illegal content, especially child pornography.
[78] *See* J. Bonnici, *Internet Service Providers and Self –Regulation: A Process to Limit Internet Service Providers Liability in Cyberspace*, available at <www.rug.nl> [retrieved 26th October 2009].
[79] *Ibid.*
[80] *Ibid.*
[81] *Ibid.*

circumstances, it is in the ISPs own interest to do so for this guarantees a certain amount of protection against liability. An ISP that does not follow the rule of its own association exposes itself to legal liability. Furthermore, AFA is strong lobby groups with government and with policy groups. It thus benefits an ISP to be a member of the association and not risk expulsion. [82]

5.3 The Law Enforcement Response

While online anonymity has attraction for the offender and poses a danger for the child, the Internet does, however, provide the potential for unprecedented paper trails for law enforcement bodies to follow and build up evidence of intent (Dixon, 2002, p. 14). This is particularly accentuated if a cyber offender communicates with a police agent posing as a teenager and sends him/her pornography. The judicial police noted that Internet investigative experts armed with appropriate technologies would be necessary to combat offenders in this complex virtual environment. It has been pointed out that familiarity with Internet practices of pedophile networks is essential to counteracting their activities online, underlying the importance of adequate funding and training and inter-service cooperation between law enforcement agencies (Dixon, 2002, p. 15). Accordingly l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication was established by the Central Direction of the Judicial Police in 2000. It targets offenders by trapping them while attempting to lure internet users. It is noted that this French Cybercrime Unit (OCLCTIC), has an online portal by which victims can report offenses and inappropriate contents on the Internet.[83] The Unit is also promoting public-private cooperation to fight cyber crime. Since 2007, l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication Commission co-organises a public- private expert meeting to discuss several possibilities of fighting cybercrime.

On October 2007 the French Police arrested more than 300 people suspected of trading in child pornography over the internet (BBC News, 2007). More than 1.4 m photographs and 20,000 videos have been seized by officers in a four-day nationwide campaign against suspected paedophiles. The investigation began after an Italian child protection group alerted police in January 2007 to a website with a link to pornographic photographs (BBC News, 2007). Police and paramilitary gendarmes identified 310 people suspected of swapping pornographic images and videos of pre-teen children online. Of those arrested, 132 have admitted to trading in child porn, while 24 others have been cleared of involvement. Dubbed "Rainbow," the police operation began on Monday and involved some 330 officers across 78 French departments (BBC News, 2007).

This year the police arrested 90 offenders in an online child pornography ring in

---

[82] *Ibid.*

[83] *See* <http://www.internet-signalement.gouv.fr/>, [retrieved 26th October 2009].

France (France Today, 2009). The roots of the operation go back to December 2004, when a site containing pornographic pictures and videos of children first came to the attention of French national police (France Today, 2009). The creator, from the northern town of Clermont (Oise), was just 17 years old at the time when he set up the site. Even though he was arrested in May 2005, the pictures and videos were still on the Net and others were downloading and sharing material from his server; proof as far as the police were concerned, that there was an "organised network in place" for diffusing child pornography. Police seized computers with one of them alone containing more than 30,000 images of young children (France Today, 2009).

5.4 Educative / Watchdog Websites

Practical measures apart from those resulting from legislative imperative have been taken by a number of ISPs and children-oriented consumer sites. Most French 'watchdog' sites provide 'safe surfing' advice tips to parents and children and crime prevention information. For example, there is the French based website *Internet – Signalement* [84] which can receive complaints and investigate them, with their main focus being on pornography.

In conjunction with the Association E – Enfance, the *Blog on E – Enfance* [85] was established to provide families, schools and the community with education and information about safe use of the Internet and has a facility to allow users to report a suspect site. It provides a forum for debate and discussion about Internet access, issues, and development.

Innocence en Danger (known as International Child Protection Movement), is part of a global network (covering over 29 countries) to promote the elimination of child prostitution, paedophilia, and other forms of commercial exploitation of children.[86] It engages in projects aimed at community education, training, awareness raising, urging law reform and effective law enforcement policies etc. It has urged Governments to make more effort to adopt a national law enforcement response to child exploitation on the Internet.

The delegation of Internet Users [87] has established a French based website Minsuers.fr, which aims at teaching children (and warning parents) about chat rooms and dangers on the Internet and to explain tactics of online paedophiles. The site contains general and technical information about chat rooms. Another French site offering similar tips and services is Internetsanscrainte.fr established under the auspices of the European Union, which seeks through providing information and technical reference, to eradicate pornography and online paedophilia on the Internet.[88]

---

[84] *See* <www.interent - signalement.gouv.fr>
[85] *See* <www.e-enfance.org/blog/>.
[86] *See* <www.innocenceindanger.org>, [retrieved 30th October 2009].
[87] *See* <http://delegation.internet.gouv.fr/>, [retrieved 30th October 2009].
[88] *Ibid.*

6. RECOMMENDATIONS

"*An ounce of prevention is worth a pound of cure*"
(Benjamin Franklin)

For those areas of the world where children have access to the Internet, especially where they have access without a requirement of supervision, it is likely that both the positive and negative effects of this accessibility will become ever more evident (Bross, 2005, p.749). Surveys of parents suggest that they buy home computers and subscribe to Internet access to provide educational opportunities for their children and to prepare them for the information-age (Subrahmanyam et al., 2001, p. 8). However, most parents' greatest fear is that their child could be a victim of sexual abuse. Consequently children are trained from early age to fear strangers. It's therefore quite a paradox that approximately 80-90% of all sexual child abuse is committed by someone close to the child.[89] In the U.S.A., a study found that (55%) of children aged 12–15 stated that they did not tell their parents everything they did on the Internet, yet adults kept an eye on children's Internet use (91%), limited online hours (62%), and used software to filter or block questionable websites (32%); moreover, two-thirds (67%) of children surveyed had to ask permission to access the Internet (Cankaya et al., 2009, p.1108). A number of recommendations for disrupting sexual abuse of children using the internet can be mentioned. Some of these recommendations will be expressed in this section.

6.1 Recommendations for National Governments

- It is recommended that policy makers acknowledge the complexity of the problem of child sexual abuse since this offense is unlikely to be efficiently prevented unless the diversity of the people who sexually exploit children or abuse them is fully taken into account.
- It is highly recommended that all national governments sign the Convention of Cybercrime and the Council of Europe Convention on Action against Trafficking in Human Beings.
- Since Internet Service Providers have vital role in protecting children on the Internet, it is thus important that governments implement legislations where self regulation of ISPs has failed.
- Justice and compensation to victims of sexual abuse remains an unresolved issue to be dealt with within a judicial system that takes account of the rights of the child.

[89] *See* T. Thea, *op. cit.* p. 65.

- National Governments should also fund research into the reactions and treatment of victims of child abuse. It is essential that governments raise societal awareness about the trauma children suffer through the production and distribution of child pornography.

6.2 Recommendations for Law Enforcement

- Resources and expertise still remain a problem in most developing countries in regard to combating child pornography and online child abuse. These resources need to be made available and co-operation with developed countries needs to be strengthened.
- Lawyers, judges and other judicial staff need training on this issue.
- The growing knowledge base amongst law enforcement agencies about child sexual abuse in relation to the Internet is welcomed. Further training of specialized child protection teams is highly recommended.

6.3 Recommendations for Internet Service Providers

- It is highly recommended that ISPs, National hotlines and law enforcement work together to fight this threat.
- It is also recommended that self – regulatory Codes of Conduct be introduced at the National and International levels on child protection.

6.4 Recommendations for Parents

- Parents should educate themselves about the Internet and the ways in which their children use it, as well as about technology in general.
- Parents should be involved in the Internet use of their children, discussing it from an early age, setting appropriate limits and instilling good behavior from the beginning.
- Parents should be attentive to at-risk minors in their community and in their children's peer group, especially because youth frequently make their risky behaviors visible to their peers**.** Helping other at-risk minors get help and support benefits all online youth.

6.5 Recommendations for Internet Community

- Members of the Internet community, including social network sites, should continue to develop and incorporate a range of technologies as part of their strategy to protect minors from harm online. They should consult closely with child safety experts, mental health experts, technologists, public policy advocates, law enforcement, etc.

As technologies designed to address safety for minors online develop, particular attention should be paid to ensuring the safety of at-risk youth, including those for

whom positive parental involvement is not a given, those for whom cost is an issue, and those who are engaged in risky behaviors and may themselves contribute to the problem.

6.6 Recommendations for Law Makers

- Law makers should develop forfeiture laws, similar to those used for drug traffickers, to seize the property of child pornographers and abusers.
- Law makers should pass legislation prohibiting the mere possession of child pornography.
- Law makers should translate their criminal codes to facilitate international cooperation.

7. WHAT THE FUTURE MAY HOLD

> *"Computer and digital technology has transformed the political economy of all pornography making it possible for almost anyone to be producer distributor and consumer simultaneously."*
>
> (Professor Liz Kelly and Linda Regan, 2000)

Child sex offenders have always used new technology to facilitate the sexual abuse of children.[90] Today, photography, videography and the Internet are used for this purpose. The Internet is the single largest source of child pornography, therefore the Internet combined with other related computer technologies promises to provide immense opportunities for the distribution of child pornography and the sexual exploitation of children, both commercially and non-commercially.[91] These technologies enable sexual predators to harm or exploit children efficiently and, anonymously. The affordability and access to global communications technologies allow abusers to carry out these activities in the privacy of their home (Hughes, 2002, p. 129). Producers of child pornography advertise their videos on the internet and distribute them through the email. Men in chat rooms trade small files, still images and short movie clips on the internet, but longer movies are sent by mail (Hughes, 2002, p. 132). Stalkers talk to children in chat rooms, ask them to take pictures of themselves, and send them through the mail. When stalkers convince children to travel to meet them, they send them bus and plane tickets through the mail. The hardest part of this section to calibrate is how the future will change the technologies that today scope both the problem and any putative solutions.

Many people actually prefer to replace reality with their own projected needs,

[90] *See* Stockholm Congress Panel Report: Child Pornography, available at <www.csecworldcongress.org>, [retrieved 29th October 2009].
[91] *Ibid.*

enjoying the emotional distance of anonymity while satisfying their sexual needs. For sexually compulsive people who seek heightened states of arousal with newer and riskier stimuli, the adult entertainment industry has already demonstrated an unscrupulous ability to deliver new material on a daily basis.[92]

Some Netizens will desire physical contact, but settle for adding a little virtual spice to their unsatisfying marriages. Others will respond to the call of the wild on the Internet, only to realize that it can awaken more than they imagined. They will try to be satisfied with seeing someone via a webcamera, but will eventually want to touch, taste, smell, and feel the body heat of their virtual lover.[93] The adult entertainment industry will develop increasingly realistic technologies to satisfy these people with "almost" the real thing, but still leave it in the virtual domain. Users of such technologies will increasingly be able to operate in a parallel world, but when that world involves high tech pornography, the Internet is a trap and will become yet another source of pain rather than a solution. Still others will start with the intention of keeping their cyber-affair limited to the Internet. When in a committed offline relationship, they will be driven to recklessly satisfy their needs, and schedule occasional face-to-face meetings with their virtual lovers. Technologies of the future will not only make electronic sexual stimulation more interactive and life-like, it will bring the experience to new levels, and more than likely foster the increased development of cyber-sexual compulsivity.[94] Aside from the influence of technology upon fidelity and children, legal issues also are likely to arise. Will the new technology establish a new form of prostitution, without the usual associated risks? "Models" viewed by videocamera can already be bought through websites. Is buying sexual stimulation over the Internet the same as having sex with a prostitute? What will be tomorrow's definition of sexual abuse? While legal limits have not yet been set on such activities, someone walking into their den is likely to have a number of responses to seeing their partner sitting at a keyboard, typing erotic requests with one hand, masturbating with the other, and watching a video conferenced male or female model performing erotic acts upon command. As our lives become more involved with technology, we must know who we are and maintain our sense of solid self as we identify our goals. The Internet is indeed seductive. It is easier than ever to slip into sexual compulsivity.

8. CONCLUSION

France has made significant progress in fighting and investigating the online sexual abuse of children and minors, most notably adopting a more collaborative

[92] *See* M. Marlene, *The Future of Cyber – Sex and Relationship Fidelity: Cyber-Sexuality*, Selfhelp Magazine, available at: <www.selfhelpmagazine.com>, [retrieved 29th October 2009].
[93] *Ibid.*
[94] *Ibid.*

approach. It must be acknowledged, however, that even that those national specialist units established in many countries are still insufficiently resourced to meet the challenges of fighting the sexual abuse of children in a virtual environment which is constantly expanding and evolving, thereby providing unprecedented opportunities for offenders. It is therefore not merely the case that successful international collaboration models such as the Virtual Global Taskforce and inter sectoral models such as that employed by OCLCTIC in France need to be extended to other jurisdictions and regions – although this is clearly a priority. On the basis of emerging trends in offending and victim behaviors, and technological developments liable to misuse, we need to be looking *now* to offending in the online environment *tomorrow*. It is thus essential to ensuring adequate child protection resources and investigative provisions to meet these increasing challenges in the coming years. Amongst specific requirements is an equivalent legislation in all jurisdictions, criminalizing all aspects of online child sexual abuse. The legislation must be accompanied by the necessary investigative and judicial procedures, capacity and resources for its successful implementation. It is also important that adults acknowledge, understand and accept the Internet and communication technology as a viable and real means of relating for children and youth in order to provide needed guidance and protection, and to keep children safe.

ACKNOWLEDGEMENT

This article was prepared for presentation at the "Lex Informatica 2009" conference, organized by Couzyn Hertzog & Horak Law Firm, S.A. Special thanks to Mr. Sizwe Snail.

AUTHOR BIOGRAPHY

Mohamed Chawki is a Senior Judge in Egypt; Founder and Chairman of the International Association of Cybercrime Prevention in Paris; Postdoctoral Fellow at the University of Aix – Marseille III; Researcher at CEDEJ (MAEE / CNRS); Senior Legal Counselor to the Minister of Military Production where he drafts legal opinions on various topics related to Information Technology and legal consultant to the Chairman of the Egyptian Financial Supervisory Authority (EFSA); member of the Consultative Section of the Ministry of Culture in Egypt and former advisor to the Chairman of Capital Market Authority (CMA). He is a regular speaker at major conferences where he has delivered over 50 conference papers and/or presentations at national and international conferences on Cyberlaw and authored many articles and chapters in books in English and French on a variety of legal topics related to IT.

REFERENCES

1. Books

Akdeniz, Y. (2008), Internet Child pornography and the Law, Ashgate, Hampshire.

Arnaldo, C. (2001), Child Abuse on the Internet: Ending the Silence, Berghahn Books, NY.

Bocij, P. (2004), Cyberstalking, Praeger, Connecticut.

Casey, E. (2004), Digital Evidence and Computer Crime, Elsevier Academic Press, California.

Chawki, M. (2008), Combattre la Cybercriminalité, Editions de Saint Amans, Perpignan.

Delmonico, D.; Griffin, E.; Moriarity, J. (2001), Cybersex Unhooked: A Workbook for Breaking Free of Compulsive Online Sexual Behavior, Gentle Path Press, Carefree.

Ferraro, M.; Casey, E. (2005), Investigating Child Exploitation and Pornography: The Internet Law and Forensic Science, Elsevier Academic Press, California.

Marsh, I; Gaynor, M. (2009), Crime, Justice and the Media, Routledge, New York.

Sheldon, K.; Howitt, D. (2007), Sex Offenders and the Internet, John Wiley, West Sussex.

Van der Merwe, D.; Roos, A.; Pistorius, T. & Eliselen, S. (2008), Information and Communications Technology Law, Lexis Nexis, Durban.

Walden, I. (2007), Computer Crimes and Digital Investigations, Oxford University Press, Oxford.

Wall, D. (2001), Crime and the Internet, Routledge, Oxford shire.

2. Journal Articles

Beech, A.; Elliott, I.; Birgden, A.; Findlater, D. (2008), "The Internet and Child Sexual Offending: A Criminological Review", Aggression and Violent Behavior 13, pages 216-228.

Bross, D. (2005), "Minimizing Risks to Children when they Access the World Wide Web", Child Abuse & Neglect 29, pages 749-752.

Cankaya, S.; Hatice, O. (2009), "Parental Controls on Children's Computer and Internet Use", Procedia Social and Behavioral Sciences 1, pages 1105 – 1109.

Doring N. (2009), "The Internet's Impact on Sexuality: A Critical Review of

15 Years of Research", Computers in Human Behavior 25, pages 1089 – 1101.

Elliott, I.; Beech, A. (2009), "Understanding Online Child Pornography Use: Applying Sexual Theory to Internet Offenders", Aggression and Violent Behavior 14, pages 180 – 193.

Hoeren, T. (2009), "The European Liability and Responsibility of Providers of Online – Platforms such as Second Life", JILT, 1.

Hughes, D. (2002), "Use of New Communications and Information Technologies for Sexual Exploitation of Women and Children", Hastings Women's Law Journal, Volume: 13, Issue: 1, pages 129 – 222.

Kierkegaard, S. (2008), "Cybering, Online Grooming, and Age play", Computer Law and Security Report, 24, pages 41 – 55.

Lievens, E. (2007), "Protecting Children in the New Media Environment: Rising to the Regulatory Challenge?" Telematics and Informatics 24, pages 315 – 330.

Mitchell, K.; Finkelhor, D.; Wolak, J. (2005), "Protecting Youth Online: Family Use of Filtering and Blocking Software", Child Abuse & Neglect 29, pages 753 – 765.

Preston, C. (2009), "All Knowledge is not Equal: Facilitating Children's Access to Knowledge by Making the Internet Safer", International Journal of Communications Law & Policy 13, pages 115 – 132.

Schell, B.; Martin, M.; Hung, P.; Rueda, L. (2007), "Cyber Child Pornography: A Review Paper of the Social and Legal Issues and Remedies – and a Proposed Technological Solution", Aggression and Violent Behavior 12, pages 45 – 63.

Stol, W.Ph.; Kaspersen, H.K.W.; Kerstens, J.; Leukfeldt, E.R.; Lodder , A.R. (2009), "Governmental Filtering of Websites: The Dutch Case", Computer Law & Security Review 25, pages 251 – 262.

Subrahmanyam, K.; Greenfield, P.; Kraut, R.; Gross, E. (2001), "The Impact of Computer Use on Children's and Adolescents' Development", Applied Developmental Psychology 22, pages 7 – 30.

Taylor, D. (2004), "Internet Service Providers (ISPs) and their Responsibility for Content under New French Legal Regime", Computer Law and Security Report, Vol.20, Issue 4, pages 268 – 272.

Wall, D. (2008), "Legal Professionalism in the Information Age", The Paralegal Educator, Vol. 22, No. 1, pages 50 – 54.

Wang, S.-J. (2007), "Measures of Retaining Digital Evidence to Prosecute Computer – Based Cybercrimes", Computer Standards and Interfaces, Vol. 29, Issue 2, pages 216-223.

Wolak, J.; Finkelhor, D.; Mitchell, K.; Ybarra, M. (2008), "Online Predators

and Their Victims", American Psychological Association Journal, Vol. 63, No. 2, pages 111 – 128.

3. Thesis

Reverdy, P.-M. (2005), La Matière Pénale à l'Epreuve des Nouvelles Technologies, University of Toulouse 1, Toulouse, un published Ph.D. Thesis.

4. Conference Proceedings

Penna, L.; Clark, A.; Mohay, G. (2005), "Challenges of Automating the Detection of Paedophile Activity on the Internet", The First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05), November 7-9, 2005, Taipei.

Quayle, E.; Loof, L.; Palmer, T. (2008), "Child Pornography and Sexual Exploitation of Children Online", The World Congress III against Sexual Exploitation of Children and Adolescents, 25 – 28 November, 2008, Rio de Janerio.

Sommer, P. (2005), "Evidence in Internet Paedophilia Cases", NCS/ACPO Conference, July 2002, Bournemouth.

5. Reports

A. Schrock and D. Boyd (2008), "Online Threats to Youth: Solicitation, Harassment, and Problematic Content", Berkman Center for Internet & Society, Cambridge.

Dixon, N. (2002), "Catching Cyber Predators: The Sexual Offenses", QLD, Brisbane.

Garlik (2008), "U.K. Cybercrime Report", Richmond.

Internet Watch Foundation (2008), "Annual Report on Cybercrime", Cambridge.

Sénat (2007), "Loi n° 2004-575 du 21 Juin 2004 pour la Confiance dans l'Economie Numérique", Paris.

Wortley, R. (2006), "Child Pornography on the Internet", U.S Department of Justice, Washington, DC.

6. Websites

Agence France Presse (2009), <http://www.afp.com>, [retrieved 12/08/2009].

BBC News (2009), <http://news.bbc.co.uk>, [retrieved 15/08/2009].

Childnet International (2009), <http://www.childnet-int.org/>, [retrieved 22/08/2009].

France Today (2009), <http://www.francetoday.com>, [retrieved 22/08/2009].

Legifrance (2009), <http://www.legifrance.gouv.fr/>, [retrieved 18/08/2009].
Second Life (2009) <http://secondlife.com>, [retrieved 07/08/2009].