

REPORT OF THE COMMITTEE
APPOINTED BY THE
BOMBAY HIGH COURT
IN
SUO MOTU
WRIT PETITION NO: 1611 OF 2001

TO
RECOMMEND MEASURES TO PROTECT AND SHIELD MINORS
FROM
PORNOGRAPHIC AND OBSCENE MATERIAL
ON THE INTERNET

January 30, 2002
Mumbai

CHAIRPERSON

Ms Archana Tyagi

DCP (Enforcement)
Crime Branch, General Branch,
CID Mumbai

MEMBERS

Dr Sourav Dutta

Videsh Sanchar Nigam Limited

Mr Vijay Mukhi

Internet Users Association of India

Inspector I M Zahid

Cyber Crime Investigation Cell,
Crime Branch, General Branch,
CID Mumbai

Mr Shashi K Nair

Advocate

Mr Gautam Patel

Advocate

NOTES TO PDF VERSION OF HIGH COURT REPORT

1. The PDF version of the Committee report dated 30.1.2002 differs slightly from the printed version submitted to the High Court.
2. The PDF version does not contain a table of contents. Instead, bookmarks are provided for navigation through the documents.
3. All URLs may not be fully converted to hyperlinks.
4. The PDF version includes a copy of the High Court order dated 13.2.2002

ADDITIONAL NOTES

1. This report is made available to the public expressly to solicit views, comments and suggestions and to enlarge the debate.
2. All comments on this report must be received within four weeks, i.e., no later than by March 30, 2002.
3. Comments may be sent :

by email to cyberreport@bombaybar.com ;	by regular mail to: Inspector I M Zahid Cyber Crime Investigation Cell, Crime Branch, CID Headquarters Opposite Crawford Market Mumbai 400 001
--	--
4. All communications, whether by email or regular mail, must contain the following particulars:
 - (a) Full name of sender
 - (b) Contact details of sender (address, telephone/fax numbers and email address)
 - (c) A brief description of the nature of the interest : whether as an individual user, Cyber Café owner/operator, ISP, etc.
5. The Committee will analyse all comments received and present the same to the High Court on April 13, 2002.

HIGH COURT ORDER DATED 13.2.2002

IN THE HIGH COURT OF JUDICATURE AT BOMBAY

O. O. C. J.

WRIT PETITION NO. 1611 OF 2001

Mr. Jayesh S. Thakkar & AnotherPetitioners

versus

State of Maharashtra & Others Respondents

—————
Petitioner – Mr. Jayesh S. Thakkar present
Mr. S. K. Nair for Respondent No.1
Mr. G. S. Patel i/b Nishith Desai for Intervenors
—————

CORAM: C. K. THAKKER, C.J. &
S. RADHAKRISHNAN, J.

DATE : 13th February, 2002

P.C. :

1. Heard the learned Counsel for the parties. In the facts and circumstances, following directions are issued:

- A. Ms. Archana Tyagi, DCP (Enforcement) Crime Branch is permitted to issue a press release (not a press conference) about the report and circulate copies of the recommendations to the press.

- B. Copies of the entire report be made available to the public for downloading on the VSNL website, the NIC website that runs the High Court daily board and the Bombay Bar Association website. The online copies of the report to be those prepared by Mr Patel, Advocate, and to be in PDF format and in HTML format.
- C. The DCP's press release and the online versions specifically to invite suggestions and comments from the public within 4 weeks; and to say that email suggestions and comments are to be sent to cyberreport@bombaybar.com (which will automatically send copies to the members of the committee); written comments and suggestions to be sent to Inspector I M Zahid, Cyber Crime Investigation Cell, Crime Branch, General Branch, CID Headquarters, Opposite Crawford Market, Mumbai 400 001.
- D. The Committee to analyse all comments and to present a summary thereof to Court within 2 weeks thereafter. Matter to be stood over for further orders till April 13, 2002.
- E. In the meantime, the measures recommended in Para 4 of Section 3 at page 66 of the report (Educational Measures) to be implemented in the first instance, under directives of the Union of India and the State Government by all ISPs.

2. At the time of hearing of the Petition, our attention was invited by the Learned Counsel for the Intervenors, Internet Users Association of India, to the order passed by the Division Bench of the High Court of Kerala in O.P. No:25463 of 2001-F dated October 15, 2001 wherein it was observed that the said Court would call for the record from the Bombay High Court so as to enable that Court to give necessary directions in that matter. In view thereof, we direct the Learned Counsel for the Internet Users Association of India to send a copy of this order along with the report of the Committee by the Bombay High Court in Suo Motu Writ Petition 1611 of 2001 dated January 30, 2002, along with annexures.

3. Parties to act on an ordinary copy of this order duly authenticated by the Associate.

sd/-

C. K. THAKKER, C.J.

sd/-

S. RADHAKRISHNAN, J.

Submitted to the Hon'ble Bombay High Court
In Suo Motu Writ Petition 1611 of 2001

Jayesh Thakker & Another
Versus
State of Maharashtra & Others
And
Internet Users Association of India (Intervenors)

COMMITTEE

CHAIRPERSON

Mrs Archana Tyagi

Deputy Commissioner of Police (Enforcement)

MEMBERS

Dr Sourav Dutta, Videsh Sanchar Nigam Limited

Inspector I M Zahid, Cyber Crime Investigation Cell

Mr Vijay Mukhi, Internet Users Association of India

Mr Shashi Kumar Nair, Advocate

Mr Gautam Patel, Advocate

SPECIAL INVITEES

Mr Jayesh Thakkar, Petitioner before the Court

Mr Sunil Thacker, Petitioner before the Court

Brig T M Sreedharan, Internet Service Providers Association of India

Mr Sudhir Gosar, Internet Service Providers Association of India

EXECUTIVE SUMMARY

- 1 Site Blocking. The Committee comprehensively rejected the proposal for site blocking as being technically and legally unsound.
- 2 Cyber Cafés. The Committee's recommendations include:
 - 2.1 A suggested definition of Cyber Cafés to be included in the Rules under the Bombay Police Act.
 - 2.2 Procedures for licensing Cyber Cafés as none are as yet licensed or regulated;
 - 2.3 Regulations requiring Cyber Café operators to demand photo id cards (of any kind) from all users;
 - 2.4 Requiring that minors be restricted to using machines in the common open space of Cyber Cafés (i.e., not in cubicles)
 - 2.5 Requiring that these machines be fitted with software filters;
 - 2.6 Providing for the maintenance of Internet Protocol address allocation time-stamped logs for all machines in the Cyber Café network.
- 3 Service Providers. The recommendations cover
 - 3.1 Requirements for maintenance of time-stamped logs of different descriptions
 - 3.2 Requirements for synchronization of internal clocks and connectivity authentication logs

- 4 Educational Measures. These include
- 4.1 Email and website information to be provided by ISPs informing the public about hazards and possible solutions;
 - 4.2 Offering filter software to subscribers as an option;
 - 4.3 Setting up a hotline to the Cyber Crime Investigation Cell;
 - 4.4 Taking steps to increase awareness about cyber crime in general.
-

SECTION 1 : BACKGROUND

1 WRIT PETITION NO:2611 OF 2001

- 1.1 On May 29, 2001, Jayesh Thakkar and Sunil Thacker wrote a letter to the Hon'ble Chief Justice of the Bombay High Court complaining about the proliferation of pornographic sites on the Internet. The letter was treated as *suo motu* Writ Petition and came to be numbered as Writ Petition 2611 of 2001.
- 1.2 During the subsequent hearings, the Internet Users Association of India (IUAI) was permitted to intervene in the matter. The Government of Maharashtra and the Union of India were also before the Court.

2 HIGH COURT ORDER DATED SEPTEMBER 28, 2001

- 2.1 On September 28, 2001, the Division Bench of the High Court, presided over by the Learned Chief Justice passed an order appointing a Committee to suggest and recommend ways, measures and means to protect/shield minors from access to pornographic and obscene material on the Internet.

3 HIGH COURT COMMITTEE

- 3.1 The High Court Committee comprised the Deputy Commissioner of Police¹; the Chairman and Managing

¹ Initially this was the DCP (Economic Offences Wing). Later, this was changed under an order of the Court to the DCP (Enforcement) since that officer had been given charge of the Cyber Crime Investigation Cell.

- Director of VSNL; Mr Vijay Mukhi or another authorised representative of the IUAI; Mr S K Nair, Advocate, and Mr Gautam Patel, Advocate.
- 3.2 The Chairman and Managing Director of VSNL was represented by Dr Sourav Dutta, the Deputy General Manager (Systems) of VSNL.
- 3.3 The High Court Order also directed that one authorised representative of the Internet Service Providers Association of India (ISPAI) and either the 1st Petitioner, Jayesh Thakker or, in his absence, the 2nd Petitioner, Sunil Thacker, would be Special Invitees to assist the Committee. The ISPAI was represented by Brig T M Sreedharan accompanied by Mr Sudhir Gosar, a technical expert.

4 MEETINGS OF THE COMMITTEE

- 4.1 The Committee met on a regular schedule at the office of the Chairperson, the DCP (Enforcement), Mrs Archana Tyagi. Meetings were held on October 8, 2001; October 17, 2001; October 24, 2001; November 3, 2001; November 7, 2001; and December 1, 2001. Minutes of these meetings are separately submitted.
- 4.2 There were also several other meetings held to approve the draft report and resolve minor outstanding issues.
- 4.3 The Committee also took the assistance of Senior Police Inspector Mr P D Pramanik of the Theatres Division. This Division is concerned with the grant of licenses under the RULES FOR LICENSING AND CONTROLLING PLACES OF PUBLIC AMUSEMENTS (OTHER THAN CINEMAS) AND PERFORMANCES FOR PUBLIC AMUSEMENT, INCLUDING CABARET PERFORMANCES, MELAS AND TAMASHAS RULES, 1960 (“the Amusement Rules”) framed under Section 33 of the Mumbai Police Act 1951. In September 2001, the Maharashtra

Government notified an amendment to the Amusement Rules introducing a definition of Cyber Cafés and also renaming the Rules themselves. The Committee has, in the present Report, proposed a definition of Cyber Cafés and suggested it to the Theatres Division.

5 THE COMMITTEE'S WORKING

5.1 Public Discussion

5.1.1 The Committee did not at any time solicit public opinion, or opinion from other ISPs or the Cyber Cafés generally. The Committee felt that the mandate of the High Court order did not permit the Committee to do so; and, going further, the Committee kept all its deliberations, minutes and drafts of this report strictly confidential.

5.1.2 However, the Committee strongly recommends that this report and its recommendations be opened to public discussion, subject to orders of the Court. This is because the subject matter of this report will inevitably affect a wide cross-section of Internet users and service providers. It is possible that such a public discussion may provide an alternative perspective on the issues at hand.

5.2 Issues

5.2.1 Based on the Terms of Reference contained in the High Court order, the issues before the Committee resolved themselves into two broad categories: Regulatory and Educational.

5.2.2 For the most part, the *regulatory issues and recommendations* cover service providers of different

hues. This is seen as an omnibus term, to include Cyber Cafés, ISPs, ASPs and online portals that provide communication services. The regulatory issues were further broken down into individual proposals, discussed later in this report.

5.2.3 The *educational issues and recommendations* deal with increasing awareness among Internet users, generally, through defined vehicles such as email newsletters, online (website) content, hotlines and help desks. There was general unanimity on these measures and proposals.

5.3 Regulatory Issues: An Overview

5.3.1 The Committee felt it was inherently impossible – or, at the very least, impractical – to evolve a common set of regulations governing all classes of service providers. Each type of service provider has its unique combination of techno-economic capabilities and limitations. For instance, online portals that provide communication platforms and solutions (email, messaging and chat) cannot assume the same responsibilities as an Internet Service Provider, which provides access to the Internet and, thereby, to all of its protocols, including those provided by online portals.

5.3.2 In analysing these individual capabilities and limitations, the Committee narrowed its focus – bearing in mind the overall objective reflected in the High Court order – to the following issues:

- (a) Blocking of sites, generally;
- (b) Preventing minors from accessing unsuitable material from Cyber Cafés;
- (c) Preventing the publication or propagation

of pornography *from* Cyber Cafés;

5.3.3 The Committee dealt separately and extensively with issues raised by Cyber Cafés. Matters related to online portals, ISPs and ASPs were considered less extensively.²

5.3.4 Regarding Cyber Cafés, the Committee further separated the general issues into subsidiary components:

- (a) Issues specifically involving minors;
- (b) Issues applicable to Cyber Cafés generally, whether used by minors or adults;
- (c) Issues relating to licensing and regulation of Cyber Cafés;

5.3.5 The report examines two issues at some length: site blocking and Cyber Cafés. These two issues occupied so much of the Committee's time because they appeared to be the focus of the Writ Petition on which the order constituting this Committee was passed; and because the order itself dwelt at length on them.

5.4 Contributions of the Committee Members

Of necessity, the Committee had to divide work among its various members.

5.4.1 **Dr Sourav Dutta**, representing VSNL, proved to be an invaluable resource on technical and technological aspects, with which he is supremely well-versed. He was able to resolve many of the

² This was because the Committee was of the view that, although the High Court order had enough play in the joints to expand the scope of the enquiry, the order clearly emphasized Cyber Cafés.

complex technical issues that came up periodically. Dr Dutta also made a detailed technical presentation to the Committee. He summarized the recommendations accurately in a specially prepared note and also clarified certain issues that the note raised.

5.4.2 Additional technical information and a presentation were provided by the Special Invitees representing the ISPAI, **Brig T M Sreedharan** and **Mr Sudhir Gosar**.

5.4.3 **Inspector I M Zahid** provided vital input regarding the working of the Police authorities, the difficulties faced by the Cyber Crime Investigation Cell, particulars of cases received by the CCIC and information about the Cyber Cafés in Bombay.

5.4.4 **Mr Vijay Mukhi** of the IUAI was able to provide the Committee with strong inputs regarding various Internet protocols and technologies. He was also an invaluable resource while assessing typical Internet usage by different types of Internet users. Mr Mukhi also read and vetted the various drafts of this report closely. He was instrumental in matching the recommendations to real-world examples to give the report more focus.

5.4.5 **Mr Shashi Kumar Nair**, Advocate, is thoroughly familiar with the complexities of the Bombay Police Act, the Amusement Rules and other applicable statutes. He was able to marshal much difficult material and draw important correlations between statutory provisions which the Committee then attempted to link to technical issues. Mr Nair was able to provide an important legal framework in crucial discussions, especially those relating to site blocking.

- 5.4.6 **Mr Gautam Patel**, Advocate, kept minutes of the Committee's meetings. He also researched and sourced additional material, legal and technical, from the Internet and other sources. He also wrote the drafts of this Report and the final report and designed its format.
- 5.4.7 Special Invitees, **Mr Jayesh Thakker** and **Mr Sunil Thacker** broadly confined their interest to issues relating to site-blocking. Their proposal was intriguing and directly triggered the extended response contained in this report.
- 5.4.8 The Committee's work would have been infinitely more difficult without the guidance, direction, focus and balance provided by **Mrs Archana Tyagi, the DCP Enforcement and Chairperson of the Committee**. Despite the pressures of her multiple assignments and tasks, Mrs Tyagi was unfailingly gracious and cheerful and was a stabilizing force, particularly when discussions became heated. She was especially concerned that the Minutes and the Report itself be an accurate record of the Committee's deliberations and, to this end, was at great pains to vet the record in minute detail. She readily engaged herself in technical and legal discussions and was able to bring these to a quick focus. When discussions sometimes strayed to a broader canvas, she was quick to point out the mandate of the High Court order. The other members of the Committee acknowledge their gratitude to Mrs Tyagi as Chairperson.
-

SECTION 2 : ANALYSIS

1 SITE BLOCKING

- 1.1 Having regard to the frame of the Writ Petition on which the order constituting the present Committee was passed, the issue of whether individual pornographic or obscene sites could and should be blocked was one of the first issues to be taken up by the Committee. The Committee was of the view that the issue required an examination of serious technical and legal aspects.
- 1.2 Before the Committee, site blocking was propounded to mean the *physical prevention of access to websites found to be pornographic*. This was vigorously canvassed by Special Invitees Mr Jayesh Thakkar and Mr Sunil Thacker.¹ As discussed later in this Report, this proposal was found to be exceedingly problematic technically and also legally. In a nutshell, the hypothesis postulates:
 - 1.2.1 that a website must be ‘found’, i.e., a roster must be kept of all websites and each must be examined thoroughly;
 - 1.2.2 that this must be done by an authorised agency;
 - 1.2.3 That agency must carry out its assessment on some objective criteria which will pass judicial scrutiny;
 - 1.2.4 The agency must then ensure that all users, throughout India, regardless of the manner in which they access the Internet, are barred from that site.

¹ Petitioners before the Court in Writ Petition No:2611 of 2001

- 1.3 The Committee expressed grave misgivings as to the techno-legal feasibility of any of these measures. No material was produced before the Committee to show that such blocking was ever found to be effective. Apart from generating controversy, it is doubtful whether such a measure has any lasting effect at all. Even in countries where it has been instituted, its effect has been limited and the measure has raised serious legal concerns. A United Nations report extracted later in this Report cites Singapore as an example where this type of 'blocking' has raised adverse legal comment.
- 1.4 On the technical aspects of the matter, one view was that site blocking was possible, at least in theory. This view was countered by the expert on the Committee, Dr Sourav Dutta of VSNL and also in part by Mr Patel, Advocate.
- 1.5 Dr Dutta demonstrated that site blocking was increasingly difficult at the ISP level. Apart from the logistical and manpower difficulties involved, it is technically impracticable. Increasingly, with the overcrowding of IP addresses, website hosts offer virtual IP addresses.
- 1.6 The overcrowding of IP addresses is well-known and widely accepted as correct. An extract from the Vicomsoft.com site² deals with precisely this issue:

In an IP network, each computer is allocated a unique IP address. In the current version of IP protocol, IP version 4, an IP address is 4 bytes. The addresses are usually written as x1.x2.x3.x4, with x1, x2, x3 and x4 each describing one byte of the address. For example, address 16843009 (hex 1010101) is written as 1.1.1.1, since each byte of this address has a value of 1.

Since an address is 4 bytes, the total number of available addresses is 2 to the power of 32 = 4,294,967,296. This represents the TOTAL theoretical

² www.vicomsoft.com/knowledge/reference/nat.html

number of computers that can be directly connected to the Internet. In practice, the real limit is much smaller for several reasons.

Each physical network has to have a unique Network Number, comprising some of the bits of the IP address. The rest of the bits are used as a Host Number to uniquely identify each computer on that network. The number of unique Network Numbers that can be assigned in the Internet is therefore much smaller than 4 billion, and it is very unlikely that all of the possible Host Numbers in each Network Number are fully assigned.

An address is divided into two parts: a network number and a host number. The idea is that all computers on one physical network will have the same network number - a bit like the street name, the rest of the address defines an individual computer - a bit like house numbers within a street. The size of the network and host parts depends on the class of the address, and is determined by address' network mask. The network mask is a binary mask with 1s in the network part of the address, and 0 in the host part.

...

[T]his means that total number of available addresses on the Internet is 2,147,483,774. Each major world region has an authority which is given a share of the addresses and is responsible for allocating them to Internet Service Providers (ISPs) and other large customers. Because of routing requirements, a whole class C network (256 addresses) has to be assigned to a client at a time; the clients (e.g.. ISPs) are then responsible for distributing these addresses to their customers.

While the number of available addresses seems large, the Internet is growing at such a pace that it will soon be exhausted. While the next generation IP protocol, IP version 6, allows for larger addresses, it will take years before the existing network infrastructure migrates to the new protocol.

Because IP addresses are a scarce resource, most Internet Service Providers (ISPs) will only allocate one address to a single customer. In majority of cases this address is assigned dynamically, so every time a

client connects to the ISP a different address will be provided. Big companies can buy more addresses, but for small businesses and home users the cost of doing so is prohibitive. Because such users are given only one IP address, they can have only one computer connected to the Internet at one time. With an NAT gateway³ running on this single computer, it is possible to share that single address between multiple local computers and connect them all at the same time. The outside world is unaware of this division and thinks that only one computer is connected.

- 1.7 This means that the trend is towards website not having unique, static IP addresses, but *sharing* a single IP address with other websites hosted on a single server machine. The trouble arises when, of this cluster of websites sharing a machine-specific IP address, one site is found to be objectionable: blocking the IP address invariably means blocking the entire machine, *including the legitimate sites*. Conceivably, therefore, a blanket recommendation for site blocking could lead to disastrous results.
- 1.8 Mr Patel pointed out that site blocking also required every ISP to constantly monitor and track all web sites and to sift through those that were acceptable and those that were not. Apart from the serious legal and constitutional repercussions implicit in any such a filtering process, it was doubtful whether any ISP had the resources to do so, given that websites keep shifting addresses⁴; and, further, that many pornographic websites do not in fact have their own domain names

³ Or proxy server

⁴ A website's domain (www.something.com) is merely a mnemonic, an easy-to-remember phrase that actually refers to a unique Internet Protocol (IP) address consisting of 12 digits grouped in threes (eg, 123.456.789.000). When a domain name or Uniform Resource Locator (URL) is entered in a browser, the domain name server of the ISP automatically translates the URL to its corresponding IP address. It is entirely possible for the registrant of a domain name to change the IP address corresponding to any web site simply by shifting the website to another computer.

but are sub-domains or virtual domains⁵.

- 1.9 On the legal aspects, Mr Patel and Mr Nair, Advocates, were of the view that any recommendation for site blocking would throw up very grave legal and constitutional questions. It involved the setting up of a separate body since, according to them, it is another dimension of censorship and could, perhaps, be an unconstitutional restriction on fundamental rights under Article 19. Mr Patel also referred to and circulated the decisions of the US Supreme Court on the matter⁶ and which had been circulated to the Division Bench. These clearly highlighted the technical and constitutional hazards of site blocking. Mr Patel was emphatic in his statement that permitting such site-blocking without any objective guidelines would amount to a conferment of uncanalised power. The Internet is a new medium and, while it brings its own set of issues and problems, equally it is not necessarily amenable to restrictions applied to earlier ('legacy') technologies and media. Inherent in the New Age of the Internet is an expanded freedom, flexibility and malleability. To strike at these is to strike at the very foundation of the medium.
- 1.10 The Committee also carefully perused the decisions of the United States District Court for the Eastern District of Pennsylvania in *American Civil Liberties Union v Reno*⁷. The *Reno I* court was addressing the Communications Decency Act ("CDA") and, while doing so, set out a comprehensive and accurate exposition of the nature of the Internet.⁸

⁵ For instance, www.someprovider.com/~somesite.com

⁶ Referred to below.

⁷ 929 F. Supp. 824 (E.D. Pa. 1996), also known as 'Reno I'.

⁸ This was on a stipulation by the parties, i.e., on an agreement between all contesting parties that this exposition was complete, accurate and relevant to the case at hand.

- 1.11 The decision carefully examines, among other things, the nature of sexually explicit material on the Internet and how it is accessed. As the decision points out, such material is seldom, if ever, accessed by accident and, usually, a series of *affirmative steps* are required to access such material.

Sexually Explicit Material On the Internet

82. The parties agree that sexually explicit material exists on the Internet. Such material includes text, pictures, and chat, and includes bulletin boards, newsgroups, and the other forms of Internet communication, and extends from the modestly titillating to the hardest-core.

83. There is **no evidence that sexually-oriented material is the primary type of content on this new medium**. Purveyors of such material take advantage of the same ease of access available to all users of the Internet, including establishment of a Web site.

84. Sexually explicit material is created, named, and posted in the same manner as material that is not sexually explicit. It is possible that a search engine can accidentally retrieve material of a sexual nature through an imprecise search, as demonstrated at the hearing. Imprecise searches may also retrieve irrelevant material that is not of a sexual nature. The accidental retrieval of sexually explicit material is one manifestation of the larger phenomenon of irrelevant search results.

85. **Once a provider posts content on the Internet, it is available to all other Internet users worldwide**. Similarly, once a user posts a message to a newsgroup or bulletin board, that message becomes available to all subscribers to that newsgroup or bulletin board. For example, when the UCR/California Museum of Photography posts to its Web site nudes by Edward Weston and Robert Mapplethorpe to announce that its new exhibit will travel to Baltimore and New York City, those images are available not only in Los Angeles, Baltimore, and New York City, but also in Cincinnati, Mobile, or Beijing -- wherever Internet users live. Similarly, the safer sex instructions that Critical Path posts to its Web site, written in street language so that the teenage receiver can understand them, are available

not just in Philadelphia, but also in Provo and Prague. A chat room organized by the ACLU to discuss the United States Supreme Court's decision in *FCC v. Pacifica Foundation* would transmit George Carlin's seven dirty words to anyone who enters. Messages posted to a newsgroup dedicated to the Oklahoma City bombing travel to all subscribers to that newsgroup.

86. Once a provider posts its content on the Internet, it cannot prevent that content from entering any community. Unlike the newspaper, broadcast station, or cable system, Internet technology necessarily gives a speaker a potential worldwide audience. Because the Internet is a network of networks (as described above in Findings 1 through 4), any network connected to the Internet has the capacity to send and receive information to any other network. Hotwired Ventures, for example, cannot prevent its materials on mixology from entering communities that have no interest in that topic.

87. Demonstrations at the preliminary injunction hearings showed that it takes several steps to enter cyberspace. At the most fundamental level, a user must have access to a computer with the ability to reach the Internet (typically by way of a modem). A user must then direct the computer to connect with the access provider, enter a password, and enter the appropriate commands to find particular data. On the World Wide Web, a user must normally use a search engine or enter an appropriate address. Similarly, accessing newsgroups, bulletin boards, and chat rooms requires several steps.

88. Communications over the Internet do not "invade" an individual's home or appear on one's computer screen unbidden. Users seldom encounter content "by accident." A document's title or a description of the document will usually appear before the document itself takes the step needed to view it, and in many cases the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content. Even the Government's witness, Agent Howard Schmidt, Director of the Air Force Office of Special Investigation, testified that the "odds are slim" that a user would come across a

sexually explicit site by accident.

89. Evidence adduced at the hearing showed significant differences between Internet communications and communications received by radio or television. Although content on the Internet is just a few clicks of a mouse away from the user, the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended.

1.12 This judgement, we were informed, was upheld by the US Supreme Court which struck down the CDA as unconstitutional.⁹

1.13 Any such blanket restriction would only reduce the efficacy of the Internet for communication, education and information, all increasingly vital and essential services today. Similar legislative attempts in America have not been accepted by the courts. An excellent article at Gigalaw.com¹⁰ by Doug Isenberg¹¹ points out, with reference to a medical issue¹² that even a statutory restriction as contemplated by the American Children's Online Privacy Act (COPA) could have resulted in an intolerable restriction on the free flow of legitimate information, including to minors. The following extract from the article highlights the hazards:

Under COPA, sites that provide "material that is harmful to minors" were required to restrict access by verifying visitors' ages with a credit card, adult access code or similar technology. Sites that failed to do so could be fined up to \$50,000 per day. COPA, however, has never been enforced, because a group of plaintiffs led by the American Civil Liberties Union filed suit to block the law immediately after it went into

⁹ *ACLU v. Reno*, 521 U.S. 844, 138 L. Ed. 2d 874, 117 S. Ct. 2329 (1997), called "Reno II".

¹⁰ <http://www.gigalaw.com/articles/2000/pfv/isenberg-2000-08a-pfv.html>

¹¹ A licensed attorney and founder of gigalaw.com

¹² Abortions, unwanted or teen pregnancies and sexual healthcare

effect, arguing that COPA would restrict *adults* from communicating and receiving information online -- a restriction that is protected by the First Amendment.

In the recent appeals court ruling, the judges agreed. Because under COPA the definition of "material that is harmful to minors" required a comparison with "contemporary community standards," and because the Internet reaches every community, the court said the only way a web site could comply with the law would be to conform with the requirements of "the most puritan of communities in any state." This forced adherence to the least-common denominator violates the First Amendment.

In other words: If COPA was the law, and if residents in the city of Maintown, USA, wanted to prevent their children from reading about pregnancy and other sex-related issues, then every web site offering that kind of information would have to create an age-verification system. My friend might then be required to provide a credit card number before she could access the free health site she found so useful after her miscarriage. And because my friend might not want to reveal her identity to read about and discuss such a personal issue, she might choose instead to stay away from the health site entirely. Fortunately, the First Amendment prevents her from having to make that decision.

- 1.14 The *concept* of site-blocking on the Internet is fraught with difficulties. It proceeds on the assumption that it is possible to define objectively and with certainty what is or is not pornographic or, at least, what is "unsuitable for minors" in an across-the-board fashion. Evidently, this is incorrect. If site blocking is viewed as a fishnet then the question is how large or small the interstices ought to be: too large a webbing allows too many to slip through; too small a webbing keeps out even the legitimate, innocuous, innocent and useful material. Testing extreme situations is bound to yield an incorrect result. It cannot, for instance, be gainsaid that a website that advocates paedophilia is unsuitable for minors. That can hardly be the test. The success or failure of any such exercise or measure must be gauged in how well it deals with a *median position*. Should minors be allowed to view a National Geographic site that has images of the

erotic sculptures of temples of Khajuraho?¹³ Should minors be allowed to see sites that deal with sex education and medical issues? Or are all these ‘unsuitable’? Are these standards rigid and inflexible for all time? Within what statutory or constitutional framework would these operate?

- 1.15 The argument that there ‘should be the creation of a fear psychosis in the minds of minors using Cyber Cafés’ was quickly rejected by the Committee. No justification for such a sweeping proposition was found or even put before the Committee. The argument seemed to proceed on a theory that all users of the Internet are irresponsible, uneducated, highly impressionable and need to have their intake of Internet material regulated by some undefined person or persons supposed to possess greater clarity, maturity and familiarity with the Internet, its hazards and benefits. The Committee felt this argument was totally bereft of merit and undeserving of further attention.
- 1.16 To arrive at any objective standard, the Committee therefore felt, was not only impossible but well beyond the purview of the present report and terms of reference.¹⁴
- 1.17 On the other hand, deployment of protective software on individual client machines (user-end machines) is a reasonable and workable solution. It is not foolproof, but affords a measure of protection. There are several excellent software products available domestically and internationally and these could well be recommended for installation on machines to which minors have access. The Committee consciously did not accept any

¹³ An example cited by US District Court in *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996).

¹⁴ The Committee was also presented with a view that the attempt should be to create a ‘fear psychosis’ in the minds of minors and others using Cyber Cafés. The Committee had no hesitation in rejecting this view unanimously.

proposal that such software be made mandatory, but only that awareness of the existence and availability of such software be increased and that it then be left to the good sense of parents as to how to limit (or not limit) their minor children's access to the Internet. If a parent does actively supervise and regulate his/her child's Internet usage, such software may not even be necessary. But, as discussed later, the Committee perceived a shortcoming in raising awareness on the issue. This is separately addressed below.

- 1.18 The Committee therefore unanimously rejected any proposal for site blocking as being technically and legally unfeasible and not salutary.

2 PROTECTING MINORS IN CYBER CAFÉS

2.1 Statutory Elements

2.1.1 The Committee found that, at present, there is no specific registration procedure for Cyber Cafés as such. A person needs only to obtain an Internet connection and set up a service in suitable premises.¹⁵ Beyond this, there appear to be no rules or regulations governing Cyber Cafés and their operation.

2.1.2 Police surveys have shown that there are 568 Cyber Cafés in Mumbai. None are regulated or licensed as Cyber Cafés specifically. None of these seem to maintain any kind of logs¹⁶ of users.

¹⁵ Subject of course to the provisions of the Shops and Establishments Act.

¹⁶ Except the Faxmen Cyber Café at New Marine Lines which maintains some logs.

2.1.3 The Government of Maharashtra and the Bombay Police have attempted to bring Cyber Cafés within the purview of the RULES FOR LICENSING AND CONTROLLING PLACES OF PUBLIC AMUSEMENTS (OTHER THAN CINEMAS) AND PERFORMANCES FOR PUBLIC AMUSEMENT, INCLUDING CABARET PERFORMANCES, MELAS AND TAMASHAS RULES, 1960 (“the Amusement Rules”) framed under Section 33 of the Mumbai Police Act 1951.¹⁷

2.2 Physical Layouts & Access to Cyber Cafés

2.2.1 The Committee also found that many Cyber Cafés have machines installed in cubicles or behind partitions, for greater privacy. This means that even minors can access and use these machines without any checks on the material that is being accessed.

2.2.2 The Committee consciously attempted to balance the need for a degree of privacy even by minors with the need to protect and shield minors from cyber pornography.

2.3 Logging and Monitoring

2.3.1 It was found that Cyber Cafés frequently use either outdated systems that are incapable of maintaining logs. Other Cyber Cafés seem to use advanced Network Address Translators (NATs), either built in to software, or in separate physical units¹⁸, or as third party software modules and/or

¹⁷ The amended definition and a renaming of the Rules were introduced by Maharashtra Government Gazette No: TICH/47-303/MBI/2001 dated September 19, 2001.

¹⁸ Called ‘black boxes’

programs.¹⁹ This means that a Cyber Café is able to split a single Internet connection between multiple users.

2.4 Effects of Lack of Control

2.4.1 The Mumbai police and the representatives of the ISPAI made it clear that due to the lack of any regulatory and enforcement mechanisms, it was virtually impossible, or at least inordinately difficult, to check and control abuses emanating from Cyber Cafés.

2.4.2 In the present scenario, it is possible to trace a miscreant *only upto the Cyber Café*. After that, it is impossible to track and find the culprit since there are virtually no records available of users, timings and machines used, and none are required to be kept by law.

2.4.3 This is what we call the “last mile” problem: A miscreant may well use Cyber Café for illegal or dangerous activities. When a complaint is received, it is theoretically possible to track the source of the offending activity upto the Cyber Café. It is, at present, impossible to track it *within* the Cyber Café itself, i.e., to find out who had used a particular machine out of the Cyber Café’s network of machines at a particular time.

Illustrations

The following illustrations are taken from actual complaints received by the Mumbai Police, Cyber Crime Investigation Cell. For obvious reasons, identities have been concealed.

A female college-going minor of around 16 was asked by a co-student to be his girlfriend. She declined and has been promptly flooded with obscene and

¹⁹ Such as software-based internet sharing systems

threatening mails. The offender has taken photos of her, obtained from a group picture, and has merged these into pornographic images downloaded from the Internet. These have been circulated to her friends accompanied by obscene and sexually explicit material suggesting that the girl is eager to have sex. These have also been sent to the girl who has abandoned college and her studies altogether and is feeling suicidal. Her parents are desperate and have asked whether they should relocate to another city. The girl is being encouraged to undergo therapy but this does not appear to be a solution. The offender has been tracked to a Cyber Café, but appears to have used more than one Cyber Café. It is impossible to find his identity from the emails.

A young lady journalist has not only received obscene mail but has had her email address revealed to others who have been told that she is sexually available. Her email box is flooded with obscene messages. The perpetrator used a Cyber Café, but cannot be identified.

A female employee of a major multinational bank found that emails were being sent, ostensibly in her name, to her colleagues, inviting them to have sexual relations with her. The offender could not be found behind the Cyber Café address.

2.4.4 Moreover, the police are hampered by Cyber Cafés being at complete liberty to offer a range of services, even to minors, completely without restrictions or limitations of any sort. This means that there is virtually no check on how minors use machines in Cyber Cafés.²⁰

2.5 Questions Addressed

The Committee was confronted with the following questions:

²⁰ The Committee did not concern itself directly with the use by minors of systems installed in homes. It was felt that this was best left to parental guidance, with suitable provisions and recommendations made to educate parents.

- 2.5.1 whether or not Cyber Cafés should be required to monitor all Internet activity on their installed networks and systems;
- 2.5.2 whether or not Cyber Cafés should be required to maintain logs of Internet activity, and, if so, to what extent.
- 2.5.3 Whether Cyber Cafés should limit minors' use of machines in some form and what this ought to be?
- 2.5.4 What physical records ought to be kept by Cyber Cafés?
- 2.5.5 What statutory and licensing mechanisms need to be introduced to provide for an adequate degree of supervision and control.

2.6 Considerations: Financial and Technical

The Committee attempted to balance the following competing concerns:

- 2.6.1 The need for privacy, even by minors;
- 2.6.2 The need *not* to create a 'fear psychosis' in the minds of minors using the Internet in Cyber Cafés.
- 2.6.3 The need to shield minors from cyber pornography.

2.6.4 The need to keep some records to assist enforcement agencies in tracking persons who abuse Internet services offered at Cyber Cafés and to provide a legal basis for the same;

2.6.5 The need to provide for recommendations that did not result in an unbearable financial burden on Cyber Cafés;

2.7 Views of the Committee

2.7.1 PHYSICAL ACCESS AND RECORDS

- (a) The Committee took the unanimous view that asking Cyber Cafés to maintain proper logs and registers of persons entering and using their facilities was feasible and desirable. The Committee has prepared recommendations on this basis. Essentially, these require Cyber Café operators to keep physical records with addresses, checked against Photo Identity cards, of persons who use their machines. Regular users can be given free ‘membership’ to obviate the need for re-entering details on each occasion. This, the Committee felt, would serve both as a check and as a deterrent.
- (b) As a corollary to the foregoing recommendation, the Committee was of the view that minors ought to be restricted to using machines that are not behind partitions or in cubicles²¹; and, preferably, are loaded with suitable checking software. The Committee was conscious that this recommendation is at some cost to the privacy available to minors but took the

²¹ That is, machines that are in the open area of cyber cafés, facing an open space.

view that the trade-off was justifiable since the restriction was limited to Cyber Cafés.

2.7.2 RETENTION OF ACCESS RECORDS: LOGGING

- (a) The discussion on this aspect was frequently heated but, ultimately, a consensus gradually emerged. Mr Mukhi pointed out that it was possible to maintain detailed logs of all activity behind the Cyber Café main server, on the Cyber Café client installations. He cited an Internet document on the subject²².
- (b) Representatives of the ISPAI took the contrary view and explained that any NAT systems is dynamic and constantly swaps port addresses every millisecond or even every nanosecond. Opening a single page often requires accessing through multiple ports, which are assigned and reassigned constantly and dynamically. This makes it virtually impossible to accurately note or log which machine was using which port at what time. This is usually done to share a single Internet connection economically among a number of machines. No material was submitted to support the view that such logging was either impractical or impossible.
- (c) On the other hand, there was a general consensus between Mr Vijay Mukhi and Dr Sourav Dutta, two technical experts on the Committee itself on this issue. They were of the view that it was *technically* possible to require Cyber Cafés to maintain automated

22

www.vicomsoft.com/knowledge/reference/nat.html?track=internal

logs of IP addresses allotted within the Cyber Café network. This log file information could be used in conjunction with a physical access record ledger or file to identify a particular offender.

- (d) The Committee preferred the view of Mr Mukhi²³, on the basis that the contrary view may well have been coloured by other considerations, technical and financial.
- (e) The Committee is conscious that this recommendation probably involves a further financial expenditure by Cyber Cafés on hardware and software, but is of the view that this is reasonable, on the basis that there is an undeniable need for responsibility and accountability when providing access to a medium that is, by its nature, so malleable, easy to use and highly susceptible to abuse.
- (f) The Committee was also clear that by recommending Cyber Café level user-logs and machine-IP logs, it was not recommending the use of any surveillance or monitoring activity or software, i.e., a log of each and every keystroke, mouse-click, transaction and Internet activity. The recommendation is limited to some form of logging that allows one to know *who* was using *which* machine at any given time.²⁴
- (g) How does this recommendation assist? Or, in other words, how is such limited logging,

²³ Especially when supported by Dr Dutta who is a senior officer at VSNL

²⁴ A proposal for maintenance of http logs allied to allocated IP addresses within the Cyber Café network was subsequently rejected by the Committee, which felt that this would not be capable of abuse but was, arguably, an unacceptable invasion of privacy.

without further detailed, every-activity-level logging sufficient to meet the needs of regulation and control? In itself, it is not sufficient; but when used in conjunction with the other recommendations for physical ids and ISP-level time-stamped logs, the accuracy of detection and tracing of miscreants is significantly increased.

Illustration

A complaint is received that an offensive, obscene email has been received by a minor. Using the ISP time-stamped logs, it is possible to trace the origin of the email to (a) the service through which it was sent and (b) the IP address from which it originated. The IP address is found to be that of a Cyber Café.

Without any of the logs, it is now impossible to tell who used the Cyber Café to send the offending email.

With only physical identification systems in place, it is possible to know that, say, 20 people were in the Cyber Café at the time indicated in the time-stamped logs. The number could be much higher.

A Cyber Café-level log would narrow down the search by pinpointing which machine had a given IP address at that time. This IP address, or other machine-specific identification, would also show up in the received email. Matching this IP address against the time logs and the physical records would then enable a process of zeroing in on the offender.

(h) A sample of the 'extended header information' available in emails shows the tracing path:

Return-Path: <vmukhi@vsnl.com>
Received: from raptor.tera-byte.com
([216.234.161.11]) by ; Sat, 19 Jan 2002 22:06:51 -
0600
Received: from mmb4.vsnl.net.in (mmb4.vsnl.net.in
[202.54.1.88])
by raptor.tera-byte.com (8.11.6/8.11.6) with
ESMTP id g0K46l155324
for <gautam@gautampatel.com>; Sat, 19
Jan 2002 21:06:49 -0700 (MST)
Received: from vijaymukhi (unknown [203.197.55.93])
by mmb4.vsnl.net.in (Postfix) with SMTP id
7B3271205F
for <gautam@gautampatel.com>; Sun, 20
Jan 2002 09:36:32 +0530 (IST)
Message-ID:
<000a01c1a167\$82c3fbb0\$5d37c5cb@vijaymukhi>
From: "vijay mukhi" <vmukhi@vsnl.com>
To: "Gautam Patel" <gautam@gautampatel.com>
Subject: High Court
Date: Sun, 20 Jan 2002 09:34:03 +0530
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="-----
=_NextPart_000_0007_01C1A195.99479990"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE
V6.00.2600.0000
X-Rcpt-To: <gasp@mcavity.com>
X-DPOP: DPOP Version 2.4a
X-UIDL: 1011505211.008
Status: U

This is a multi-part message in MIME format.

-----=_NextPart_000_0007_01C1A195.99479990
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

- (i) This information, embedded in all email²⁵ tell us that an email was sent by Mr Vijay Mukhi who, when connected, had an IP address 203.197.55.93. The mail was sent through the VSNL bom4 (mmb4) server with an IP address of 202.54.1.88. The time and date are also given. This means that the email can be accurately tracked to Mr Mukhi. If the first IP address, 203.197.55.93 is that of a Cyber Café, then it is not possible to know who in that Cyber Café sent the email. To know that, a *further, internal* IP address assigned by the Cyber Café server to all its networked machines would have to be provided, logged and made available for inspection against a physical time-stamped log.
- (j) This requirement actually works to the benefit of minors both within and outside Cyber Cafés. It allows one to know whether minors are being permitted by Cyber Café operators to access unsuitable material and to play mischief; and it protects minors from harassment by persons using Cyber Cafés, whether or not the minor is himself or herself using a Cyber Café.
- (k) The Committee therefore concluded that the use of NATs and similar technologies²⁶ must be accompanied by suitable logging protocols; and, further, that, NAT (or similar) logs should be maintained for a

²⁵ Or which *should* be embedded in all email; there are some providers that suppress this information.

²⁶ Such as Port Address Translators (PAT)

minimum of three months.²⁷

2.7.3 LICENSING AND STATUTORY DEFINITIONS

- (a) The Committee considered and extensively recast the proposed definition of Cyber Cafés in the *Amusement* Rules under the Bombay Police Act.
- (b) The Committee attempted a definition that was sufficiently broad to cover all forms of Internet use but specifically excluded private installations in residences and private offices.
- (c) The Committee was also aware that Cyber Cafés frequently offer Internet access services gratis, but bundled with the purchase of other goods or services, typically refreshments. The Committee's definition therefore attempted to cover such situations also.
- (d) The Committee also reworked an application form²⁸ that is *required* to be filled in, and permission obtained thereon from the Police Commissioner, for opening a Cyber Café. Existing Cyber Cafés would have to apply on the same form for a license. Failure to get a license invites consequences, including prosecution and closure, contemplated under the *Amusement*

²⁷ There was also a proposal that the browser history lists, i.e., lists of websites visited by users in cyber cafés, should be retained. This was rejected because it is possible to wipe out these lists in a matter of seconds and can even be done accidentally by a user; but more importantly because it is, perhaps, an unconscionable encroachment on privacy and constitutional freedoms.

²⁸ A corresponding change is also recommended to the license form of every ISP; and to the application form taken by every ISP from a prospective cyber café operator.

Rules.

3 PREVENTING PUBLICATION FROM CYBER CAFÉS

- 3.1 A distinct aspect of the matter involved the use of Cyber Cafés to publish or propagate pornography.
- 3.2 Strictly speaking, this is not limited to the use by minors, but is at a broader level.
- 3.3 Publication and transmission of pornography is an offence under the Information Technology Act, 2000²⁹.
- 3.4 Usually, such publication would be done using File Transfer Protocol (FTP), for which various software products are readily available. FTP allows the movement of a large number of files, and large sized files, between a local client machine to a remote server³⁰ at a rapid speed. An early view was that FTP access from Cyber Cafés ought to be blocked. This view was rejected when the Committee found that, especially in areas outside Bombay, FTP is regularly used by students and professionals³¹ to transmit large files.
- 3.5 The Committee therefore accepted that FTP access could continue from Cyber Cafés but, conscious of the need to control the use of FTP, recommends that FTP logs be maintained for a period of at least three months. These logs do not need additional hardware or even software³²; and the additional software, if required, is

²⁹ Section 67.

³⁰ Often located overseas and therefore beyond jurisdiction.

³¹ Particularly in engineering and sciences

³² Logging features are built in to most industry-standard FTP software packages.

affordable.

4 **ONLINE SERVICE PROVIDERS – LICENSING & DEFINITIONS**

- 4.1 The issues with regard to Service Providers essentially centred around logging and maintenance of internet access records.
- 4.2 The Committee found that there were several distinct types of service providers:
- 4.2.1 Internet Service Providers such as VSNL, which have direct access to the Internet, which they then give out to subscribers³³ or Internet Access Providers.
- 4.2.2 Internet Access Providers such as InCable, Hathaway, etc., which obtain bandwidth from ISPs and then give these out to subscribers³⁴
- 4.2.3 Online Service Providers which do not provide connectivity but offer free or paid online services such as chat, email, messaging, etc. Examples include Hotmail, Yahoo, Rediff.com, Indya.com and other services.
- 4.3 The Committee was of the view that all these are Network Service Providers within the meaning of the IT Act, 2000³⁵. The Committee suggests that an amendment to this effect be incorporated in the IT Act by the Central Government and that a recommendation to this effect be made by this Hon'ble Court. This will

³³ Including cyber cafés.

³⁴ Including cyber cafés.

³⁵ Section 79 read with Section 2(w), definition of 'intermediary'

make the NSPs accountable under the provisions of the IT Act.³⁶

- 4.4 Needless to say, these provisions will apply only within local jurisdiction, i.e., to those service providers who are based in, or have their servers located in, India.

4.5 Records Keeping

4.5.1 The lack of proper time stamps and the maintenance of time-stamped records makes it very difficult for enforcement agencies to track perpetrators of cyber crimes generally. The Bombay Police informed the Committee that it has great difficulty in obtaining suitably time-stamped records from NSPs. Many email providers, for instance, do not maintain time stamps, or their clocks are not properly synchronised.

4.5.2 Given that all NSPs have expensive installations, the requirement of maintaining adequate time stamps on outbound email was felt to be reasonable.

4.6 Connectivity and Authentication

4.6.1 Whenever a computer connects to the Internet, through an ISP's systems and the gateway, it is assigned a unique IP address. This may either be a static IP address, i.e., one that is unique to each subscriber (but is expensive to maintain and limits the number of subscribers) or a dynamic IP address. A dynamic IP address, as the name

³⁶ Section 79 provides that NSPs are liable where they cannot demonstrate diligence or lack of foreknowledge in case of any violation of their service.

implies, changes per connection. This means that a single user has one IP address when he first connects; and, possibly, an altogether different IP address when he disconnects and reconnects.

4.6.2 Static IP addresses have the advantage of uniquely identifying the subscriber. By the same token, however, they are significantly more susceptible to hacking and attacks since the IP address of the subscriber remains constant and can be detected either by a hacker or even automatically by malicious code. To this extent, dynamic IP addresses provide a degree of security to the subscriber clients.

4.6.3 The difficulty with dynamic addresses is being able to correlate the subscriber's telephone number³⁷ with the IP address assigned when the connection is made. With a static IP address, this is not a problem. With dynamic IP addresses, it is very difficult. The difficulty is compounded when the ISP does not

- (a) Maintain authentication and usage records;
- (b) Does not have the Automatic Number Identification³⁸ feature set on its Remote Access Server.

4.6.4 The Bombay Police have therefore great difficulty in tracking cyber-felons since they cannot find the telephone number or the IP address of the connection or cannot match the two. Many ISPs do not maintain logs, or maintain them for insufficient periods.

4.6.5 Many of tracking and detection issues would be

³⁷ The number *from* which the subscriber has dialed in to the ISP modem or server

³⁸ similar to the Caller Line Identification Protocol (CLIP) or "Caller ID" as it is popularly known, offered by MTNL.

resolved by compelling the maintenance of non-repudiable authentication and usage records. This means that whenever a subscriber dials in³⁹, the ISP should have an automatic logging of the telephone number from which the dial up connection is initiated, along with the IP address assigned.

4.6.6 This has two implications. Firstly, it means that no anonymous connections should be given to the subscriber. As regards broadband users, it is suggested that, for this as also for security reasons, the connection be restricted either to the cable modem ID, the network card adapter address or the processor chip ID, all of which are unique. This prevents others from using the subscribed broadband connection.

4.6.7 To facilitate record auditing and tracking, it was suggested that these remote access user logs⁴⁰ be kept on some reliable removable media for permanent storage and retrieval, , and may be in compressed form to conserve space, e.g. CDR media etc.

³⁹ Or in the case of a broadband connection, turns on his machine or logs in

⁴⁰ RADIUS or Remote Access Dial In User Service/Server

5 PHOTO IDS IN CYBER CAFÉS: PUBLIC OPINION

- 5.1 The Committee was aware that there has been some debate on the Internet about the propriety or suitability of compelling the use of Photo ID cards for accessing Cyber Cafés. The move to introduce these cards has been widely questioned in the media and elsewhere.
- 5.2 An instance of a critical article is one featured on the Naavi.com website (www.naavi.com), entitled *The Dilemma of Id for Cyber Café ... Fit Case for a Big Debate*.⁴¹ This article criticizes the move by the Bombay Police to force the use of Photo ID cards in Cyber Cafés.
- 5.3 Given that the Committee has accepted this proposal, the Committee thought it appropriate to present its view and allay the fears expressed in the *Dilemma* article.
- 5.4 The article states that the threat of cyber crimes from Cyber Cafés is so miniscule as not to justify the ID card measure. This appears to beg the question. Firstly, the article acknowledges that cyber crimes *are* being committed from Cyber Cafés, but gives no material to support the stand that these are miniscule. Even assuming this to be so, there is no justification to *not* taking what is evidently a pro-active measure. To wait till the volume of cyber crime is serious and *then* to introduce the measure is rather like shutting the stable door after the horse has bolted. With an inherently malleable, open and free medium like the Internet, it is entirely possible to abuse its features against the interests of the nation.
- 5.5 That may be a larger canvas than is presently warranted. But the current Terms of Reference require that measures be taken to curb the exposure of minors to indecent materials. A simple, effective, low-cost and flexible solution is presented by the ID card proposal. In

⁴¹ http://www.naavi.com/cl_editorial/edit_01May20_01.html

fact, the proposal is eminently in the interests of Cyber Café operators, minors and parents. An unaccompanied minor in a Cyber Café puts the Cyber Café owner or operator *in loco parentis*, to the extent that the minor is being permitted to access and use the Internet. This could have serious legal repercussions. The ID card proposal actually serves to limit the exposure of the Cyber Café owner and provides him with a means to control abuse and damage within his enterprise.

- 5.6 The article also speaks of enforcement problems and says, in substance, that the requirement will be ignored. This is a valid point, to an extent; it only means that if a Cyber Café operator, faced with the requirement of checking ID cards, does not do so, and a cyber crime is committed from his enterprise, then a legal provision must be made to provide for his prosecution or penalty.
- 5.7 The *Dilemma* article claims, lastly, that the measure infringes the “right to privacy” or some (unspecified) freedom. This argument appears to be untenable and, in the manner in which it is couched in the *Dilemma* article, is needlessly alarmist. The Committee was at all times fully conscious of constitutional and legal limitations and saw no reason to introduce more invasive mechanisms. The ID card proposal does nothing more than to require a user to confirm that he is who he says he is; and to note his address. In the case of minors, the Committee feels this is essential. There is no way to assist a minor or guide his parents if the parties do not even know who that child is or where he stays. This is a far cry from the Orwellian scenario envisaged in the *Dilemma* article, which fears that tabs will be kept on *all* movement of an individual. We ask that it be noted that the ID Card proposal does not restrict use of the Internet *per se*; its intention is merely to screen out the malcontents and miscreants bent on abusing what should be a safe, educational, informative, profitable and valuable medium.

6 EDUCATIONAL MEASURES

- 6.1 The Committee fully accepted that education of parents and minors was possibly the best way to protect minors from unsuitable material on the Internet.
- 6.2 The Committee found that there is, in fact, no concerted, effective or regular effort being made by any ISP in this direction. Most ISPs send out regular email newsletters and have their own websites⁴². These do not contain information about cyberpornography, cybercrimes, the hazards to minors or suggestions of measures that can be taken.
- 6.3 The Committee views this as an extremely serious lacuna in the working of ISPs and ASPs. It is the view of the Committee that merely providing access, or speedy access, to the Internet is not a sufficient discharge of the obligations and duties of any ISP. Given the inherent dangers and hazards of the Internet, it is incumbent on every ISP to take pro-active steps to alert and inform their subscribers. The Committee is of the view that there are a number of simple and inexpensive measures that can be taken by ISPs in this regard, including putting out special email bulletins, holding seminars, providing information online and offline (via telephone calls) and coordinating with the Mumbai Police's Cyber Crime Investigation Cell.
- 6.4 The Committee also feels that every subscriber should be offered the choice of downloading control software, i.e., software that can be installed on the subscriber's machine to restrict minors' access to objectionable sites.

⁴² For example, VSNL: <http://internet.vsnl.com>; Satyam: <http://www.sify.com>; Rolta: <http://www.roltanet.com>; TataNova: <http://www.tatanova.com>; NetKracker: <http://www.netkracker.com>

This is machine-level blocking⁴³. Almost all ISPs offer software on CDs when a subscription to their service is taken. The Committee feels that a suitable protective software could be included in the CD package, the price being built in to the subscription. Subscribers would have the choice of installing or not installing the software; but at least they would not be driven to having to purchase the software from an international site using their credit cards online. There are several excellent packages readily available, such as, amongst others, Net Nanny, Cyber Patrol, SafeSurf, SurfWatch, CyberSitter, etc.⁴⁴

- 6.5 The Committee has prepared recommendations on this basis, and also recommended measures for coordination with the Mumbai Police.

7 THE EFFECTS OF CYBERPORN ON MINORS

- 7.1 This analysis would be incomplete without at least a brief overview of the effects of cyber pornography on minors. The Committee fully appreciates that these dangers are inherent, implicit and so widely acknowledged as to warrant no further restatement. Nonetheless, the Committee was of the view that the issue needs to be put into some factual context and not merely rest on a theoretical or assumptive foundation. This is because the report has been called for by the Hon'ble Bombay High Court and also because it may well be debated in the public media.

⁴³ And cannot be 100% guaranteed, but sufficiently serves to protect minors from unsolicited material being thrown at them.

⁴⁴ In *Reno I*, *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996), the US District Court reviewed some of these software packages and their functionality.

- 7.2 On October 16, 1997, the Secretary General of the United Nations presented to the General Assembly a report on the sale of children, child prostitution and child pornography prepared by Ms. Ofelia Calcetas-Santos the Special Rapporteur of the Commission on Human Rights in accordance with General Assembly resolution 51/77. This report is available online.⁴⁵
- 7.3 While the report deals with the sale of children, child prostitution and child pornography generally, it also contains a precise delineation of the problems associated with the Internet. It says, “Children who are exposed to pornography are in danger of being desensitized and seduced into believing that pornographic activity is ‘normal’ for children. It can provide a kind of modelling that may adversely affect children’s behaviour and result in learning experiences which connect sex to exploitation, force or violence.” While the entire UN report is appended to the present report, the following passage is extracted to highlight issues that are immediately relevant:

5. New media: the role of new technologies in the commercial sexual exploitation of children

78. First, the nature of technology: it is a great blessing, and what do we know about blessings? That every blessing has its curse. The greater the blessing, the nastier the curse. Technology has the tendency to separate people from the consequences of their worst behavior.”

79. The Internet is a giant network of networks. It is virtually impossible to determine its size at any given moment, but it has grown massively since its origins as an experimental project linked to defence-related research in 1969. In 1981, fewer than 300 computers were linked to the Internet but, by 1996, it was estimated that 9.4 million host computers were linked, 60 per cent of them located in the United States. Reasonable estimates suggest that as many as 40 million people around the world can and do access

⁴⁵ At <http://www.hri.ca/fortherecord1997/documentation/genassembly/a-52-482.htm>

the enormously flexible communication medium. That figure is expected to grow to 200 million Internet users by the year 1999.

80. The Internet is in a unique position to take advantage of new technology, as text, photographs, video and audio clips can be disseminated worldwide instantly. The most constructive ways in which it can be used to tackle the commercial sexual exploitation of children include using the new technology to further expand and develop methods of communication and education for the prevention of such exploitation. However, the virtually inexhaustible categories of information which the Internet can provide include innovative and simplified means of sexual exploitation.

81. The problem of accountability. The Internet is a decentralized, global medium of communications known as "cyberspace" that links people, institutions, corporations and Governments around the world, and the computer networks are owned by governmental and public institutions, non-profit organizations and private corporations. No single entity, academic or governmental, corporate or non-profit, administers the Internet. There is no central point at which all the information is stored or from which it is disseminated, and it would not be technically feasible for any one entity to control all of the information conveyed on the Internet.

82. The risks to children on-line. While the Special Rapporteur recognizes and commends the educational value, especially for developing countries, of the wealth of information available on the Internet, there are many ways in which children may be exposed to danger on-line. The two main ways in which children may potentially be harmed by child pornography are by being exposed to pornography and by being filmed or photographed or made the subject themselves in some other way.

(a) The child as viewer

83. Children who are exposed to pornography are in danger of being desensitized and seduced into believing that pornographic activity is "normal" for children. It can provide a kind of modelling that may adversely affect children's behaviour and result in learning experiences which connect sex to exploitation, force or violence.

84. There have been some highly publicized cases of abuse involving computers but reported cases are relatively infrequent. Like most crimes against children, many cases go unreported, especially if the child is engaged in an activity that he or she does not want to discuss with a parent. Teenagers are particularly at risk because they often use the computer unsupervised and because they are more likely than younger children to participate in on-line discussions regarding companionship, relationships or sexual activity. These risks include exposure to inappropriate material of a sexual or violent nature, or encountering e-mail or bulletin board messages that are harassing, demeaning or belligerent. Another risk is the possibility that, while on-line, the child may provide information or arrange an encounter that could risk his or her safety or the safety of other family members. In a few cases, paedophiles have used on-line services and bulletin boards to gain a child's confidence and then arrange a face-to-face meeting.

Restricting access to unwanted on-line material

85. Various manufacturers have begun to build systems and have marketed software intended to enable parents to control the material which comes into their homes and may be accessed by their children, allowing them to enjoy the educational benefits of the Internet while shielding them from material that is objectionable according to the parents' own particular standards.

86. Some software manufacturers have started to employ people to search the Internet for sites containing potentially offensive material, which they then add to a list every week. For those users who have the relevant software installed, the updated elements are automatically added to the list of previously blocked sites.

87. Other types of programs allow a parent to monitor everything passing through their computer. Parents can enter such phrases as "What's your name?" and "What's your phone number?" in a phrase book. When the software detects one of the targeted phrases printing across the terminal, for example in a chat room of a commercial on-line service, it immediately logs off the service.

Content on the Internet

88. The types of content on the Internet defy easy classification, and can be as diverse as human thought. Such diversity is possible because the Internet provides an easy and inexpensive way for a speaker to reach a large audience, potentially of millions. Any Internet user can communicate by posting a message to one of the thousands of news groups and bulletin boards or by engaging in an on-line "chat", and thereby reach an audience worldwide that shares an interest in a particular topic.

89. Because of the different forms of Internet communication, a user of the Internet may speak or listen interchangeably, blurring the distinction between "speakers" and "listeners" on the Internet. Unlike traditional media, the barriers to entry as a speaker on the Internet do not differ significantly from the barriers to entry as a listener. Once one has entered cyberspace, one may engage in any dialogue that occurs there.

Sexually explicit material on the Internet

90. Sexually explicit material includes text, pictures and chat between users. It includes bulletin boards, news groups, and the other forms of Internet communication, and extends from mildly titillating to hard-core pornography. Although surveys done by on-line administrators suggest that pornographic sites are among the most often used on the Internet, the percentage of such sites is not certain. Once a provider posts material on the Internet, it is available to all other Internet users worldwide, and the provider cannot prevent that content from entering any community. The Internet technology gives a speaker a potential worldwide audience, although almost all sexually explicit images are preceded by warnings as to the content.

Identity of Internet users

91. It is impossible to determine conclusively the identity or age of a user accessing material through the Internet. An e-mail address may comprise an alias or use an anonymous re-mailer. There is also no universal listing of e-mail addresses with corresponding identities, and any such listing would rapidly become incomplete. A sender therefore has no way of knowing whether an e-mail recipient is an adult or a minor. Similarly, even individuals engaging in chat room discussions cannot ensure that all

readers are adults.

92. Even if it were possible with the available technology to block access for children to certain news groups or chat rooms, there is no method by which the creators of news groups that involve discussions of normally acceptable subjects such as art or politics, but could potentially elicit indecent contributions, could limit the blocking of access by minors to the indecent element only, while still allowing them access to the remaining content. Even security systems such as credit card verification or adult password verification are unlikely to develop the capacity to ascertain that the user of the password or credit card is over 18.

93. Therefore, all speech on any topic that is available to adults will also be available to children using the Internet, unless it is blocked by screening software running on the computer the child is using. It is not possible for a speaker using current technology to know if a listener is using screening software.

94. The attempts to regulate children's access to pornography by the development of software programs, although very welcome, cannot achieve more than a very limited success, as these programs can be bypassed by users with a good knowledge of the Internet and some technical sophistication. Even if better technical solutions become available, this approach is inadequate because children can increasingly find access to another computer, and their technical expertise is often far superior to that of their parents.

Anonymity

95. Anonymity is important to Internet users who seek to access sensitive information. A user can invent virtually any identity and route a message through different countries so that when it reaches its destination it will be impossible to determine its origin. It is also possible to re-route e-mail and images through what are referred to as "anonymous re-mailers". These take incoming messages and remove the source address, assign an anonymous identification code number with the re-mailer's address, and forward it to the final destination. Responses to the anonymous messages are then similarly encoded and the responder also remains anonymous. In Finland, one such re-mailer service

used to be operated by Johan Helsingus, who, however, closed down the service after being accused of paedophilia, which he strongly denied. An adverse repercussion of the close-down was suffered by the British organization The Samaritans, which counsels people contemplating suicide and has increasing numbers of computer contacts, many of whom use the "re-mailer" service to remain anonymous.

(b) The child as material

96. The advances in computer technology, including the use of camcorders, VCRs, home-editing desks, computer-generated graphics and editing, have made the creation and distribution of child pornography easier, cheaper and more difficult to detect. It has developed into a multi-million-dollar industry which can be run from within the exploiter's home.

97. Every photograph or videotape of child pornography is evidence of that child's abuse. The distribution of that depiction repeats the victimization over and over again, long after the original material was created. A case in point is the death by suicide of a 12-year-old boy in Upper Austria, who killed himself after discovering, in addition to the trauma of being sexually abused by an older man, that photographs of those abusive acts had been posted on the Internet.⁴

98. Images can be altered by computer. It is not difficult to add to an image or delete parts of it, thereby creating pseudo-photographs. A child's face can be superimposed on an adult's body, and adult features such as breasts and genitals can be minimized so as to make the images look like children. The distribution of the altered image is still considered to exploit the child whose face is shown. It is also possible to insert digital images of a person into a video in which he or she has not appeared. Life-like child pornography is now being created without using any real children at all.

99. There are an increasing number of cases of child pornography being reported which do not involve visual images. An unusual legal situation arose following the arrest of 19-year-old Joseph Pecchiarich in Mississauga, Canada, in 1993. He became the first person in Canada to be convicted of distributing child pornography via computer, but he had never photographed or filmed actual children. He wrote and

posted on the Internet several stories which depicted himself having sex with several female children, who were always portrayed as willing partners. He was arrested for distributing child pornography, which under Canadian law is defined not only as materials involving real children, but that which depicts children involved in sex, or advocates sex with a child under the age of 18. He was charged under section 163.1, which was debated in parliament as bill C-128, and became law on 1 August 1993, amending the Canadian Criminal Code. One of the ideas behind the law is that the harm caused by child pornography extends beyond the direct abuse of children in its production and that such material has great potential to promote child sexual abuse whether the child portrayed is a real person or not.

100. The Internet can be used by paedophiles to contact each other and they can set up bulletin boards to exchange information relating to their sexual interest in children, or have running conversations in the form of chat rooms on such subjects.

101. For those who would seek to access images of child pornography through the Internet, a basic search using the most obvious keywords such as "child pornography" will normally direct the user towards sites campaigning against the Internet being used as a medium for the distribution of such material, or news items relating to the arrests of those suspected of being involved. Many non-governmental and private organizations and individuals are starting to voice their fears for the future of the information superhighway, and much research is being carried out to consider the best ways to tackle the problem.

102. Unfortunately, even the extensive and ever-increasing collection of well-meaning initiatives, studies and surveys into the nature of the problem and possible ways to approach a solution have not escaped allegations of abuse. **An example of this is the controversy surrounding the "cyberporn" study of Marty Rimm of Carnegie Mellon University. The ethics of the study, entitled "Marketing pornography on the information superhighway", which purported to analyse the amount and nature of pornographic materials being posted on the Internet, have been called into question, as the study involved looking for pornography,**

downloading it, and studying how it had been classified. Criticisms of the way the research was carried out included accusations of invasion of privacy, deception, placing human subjects at risk, and possible fraudulent data gathering. It was also alleged that the study was a deliberate search for child and teen pornography.

C. National and international initiatives

103. **Two possible means to prevent child pornography from being posted on the Internet are the legal system and self-regulating initiatives. As the development of the Internet is still in its infancy, Governments that have attempted to regulate its use have often not fully understood either the technology or the implications of their actions to control it. Self-regulating initiatives, which give the users of the Internet some responsibility over what should be removed, have made some progress towards removing the conflict between regulation and freedom of expression.**

104. In the Netherlands, the Hotline for Child Pornography on the Internet was created by the Foundation for Internet Providers, Internet users, the National Criminal Intelligence Service, the National Bureau against Racial Discrimination and a psychologist. Like other national hotlines that are starting to be set up, it operates by asking Internet users to report any child pornography that they find. The Netherlands Hotline tries to have a preventative attitude towards the problem, in that once a site is reported, the Web Site provider will ask the issuer of the material, if he can be traced, to remove it from the Internet, and will report that person to the police if he or she fails to do so.

105. The hotline has also tried to raise awareness of the risks of spreading child pornography, including the fact that the penalty in the Netherlands is four years' imprisonment. Much attention has been given to the hotline by the media, thus further stimulating the process of awareness and prevention. Instead of being censors, such hotlines are intended to be regarded as initiatives against censorship, by indirectly targeting the poster of illegal child pornography instead of whole areas of information and communication.

106. **In India, the Government has attempted to prevent misuse of the Internet by limiting access to the service to the academic world. As a result, the Internet remains inaccessible to the individual or commercial user.**⁴⁶ Similarly, the entry of foreign print and electronic media into the country has provoked a controversy, with the Government still undecided about its stand.

107. Singapore has attempted to regulate the content of the Internet as far as possible, through a Class Licence Scheme, where Internet service providers and Internet content providers are required to block out objectionable sites as directed by the Singapore Broadcasting Authority. Schools, libraries and other providers of Internet access to children are required to institute a tighter level of control, although options as to how this could be implemented have not yet been identified. **The Special Rapporteur has learned that concerns have been expressed as to the scope and vagueness of the Internet content guidelines and the effect that they might have on the Singaporean right to freedom of expression.**

108. **In China, Internet users must register with the police, and it is reported that a company in Massachusetts, United States, is investing in technology designed to allow the Government of China to censor the Internet.**

109. The Internet Society of New Zealand and the Internal Affairs Department set up a joint working group to tackle pornography on the Internet in December 1996. This followed several high-profile raids and monitoring exercises by the authorities. **The Society is also developing a code of practice for Internet service providers.**

110. In connection with the first World Congress against Commercial Sexual Exploitation of Children held at Stockholm in August 1996, the Norwegian Ombudsman for Children and Save the Children Norway initiated a project with the aim of identifying paedophile networks: systems, methods, codes and ways of communication used by criminals involved in the sexual exploitation of children. Extensive investigations undertaken by professional computer hackers revealed organized trading in child

⁴⁶ This is no longer true.

pornography on the Internet, and special sites containing information on sex tours and meetings. In one chat group hard-core amateur child pornography was found, showing girls and boys between the ages of 8 and 12 being raped repeatedly by adults of both sexes.

111. ...

112. In the United States of America, the Supreme Court recently ruled that a federal law which sought to curb indecency on the Internet was unconstitutional.⁴⁷ The plaintiffs, who included various organizations and individuals associated with the computer and communications industries, and those who publish or post materials on the Internet, challenged on constitutional grounds provisions of the Communications Decency Act of 1996. They contended that two provisions of the Act directed to communications over the Internet which might be deemed "indecent" or "patently offensive" for minors, defined as persons under the age of 18, infringed upon rights protected by the First Amendment and the due process clause of the Fifth Amendment, in that adults would be denied access to materials which they had the right to see.

113. Since the Internet crosses state and national boundaries, Internet users must be careful that they avoid violating not only the federal laws and their own state laws, but those of any other State which might become involved. In one famous case, Operation Longarm, United States authorities, with the cooperation of the Government of Denmark, tracked down the identity of callers from the United States who downloaded child pornography from a Danish bulletin boards (see E/CN.4/1997/95/Add.2). The United States Customs services then raided the homes of the suspected callers and confiscated their computers, floppy disks and other materials. Several people were prosecuted as a result.

⁴⁷ Reno II. *ACLU v. Reno*, 521 U.S. 844, 138 L. Ed. 2d 874, 117 S. Ct. 2329 (1997).

114. The United Kingdom police were involved in Operation Starbust, an international investigation of a paedophile ring thought to be using the Internet to distribute graphic pictures of child pornography, and the biggest operation so far carried out in the United Kingdom. Nine British men were arrested as a result of the operation, which involved other arrests in Europe, America, South Africa and the Far East. The operation identified 37 men worldwide.

115. Also exposed during Operation Starbust was Father Adrian Mcleish, 45, a Roman Catholic priest in Durham who held the largest known collection of illicit matter yet gathered electronically. He had amassed a vast store of obscene pictures and drawings in his presbytery and exchanged thousands of explicit e-mail messages with other paedophiles. He was sentenced to six years' imprisonment in November 1996. He admitted 12 specimen charges of indecent assaults against two boys of 10, one aged 12 and another aged 18. He also admitted distributing indecent photographs, possessing them with intent to distribute them and being involved in the importation of pornographic videos of children. There was evidence that he had sent pictures of at least one of the boys he had abused and talked on the Internet of "grooming" the boy for use in later life. He had also enhanced some pictures to make them more sexually explicit.

- 7.4 Para 109 of the report cites China. This was also the subject of a recent article in the press and online⁴⁸, where it was reported that China had closed several thousand Cyber Cafés.⁴⁹ A closer scrutiny led us to believe that the exercise was more driven by political than social concerns.
- 7.5 The Committee considered other material, too, while addressing the issue. Much of this was taken from the Internet itself. This report includes a select bibliography. One report, however, merits special mention in addition to that of the Special Rapporteur to the United Nations. This is a paper of April 16, 1999 by Professor Nicholas

⁴⁸ <http://dfn.org/focus/china/internetcafes-closed.htm>

⁴⁹ A copy of the online article is annexed to this report.

Johnson presented at the Cyberspace Law Seminar at the Misook Baek School of Journalism and Mass Communications of the University of Iowa. The paper entitled “THE INTERNET AND PORNOGRAPHY: IN THE SEARCH FOR REGULATORY ALTERNATIVES IN A NEW TECHNOLOGICAL ENVIRONMENT”, is available online.⁵⁰

- 7.6 The paper contains a comprehensive review of the judicial and legislative attempts made in the past to ‘control’ and ‘regulate’ the Internet and also examines certain influential papers written on the subject⁵¹. Among the recommendations in the paper are those related to cyber-zoning, a concept that was also enunciated by Justice Sandra Day O’Connor of the US Supreme Court in the *ACLU* case⁵². The following extract is culled from the paper:

V. Two Alternatives: Contemporary Standards of Obscenity and Cyber Zoning

Debate surrounding pornography has produced extreme controversy between different political and ideological camps, and regulation of pornographic content on the Internet is magnifying this conflict. Absolute free speech groups, including anti-censorship feminists and libertarians, unwillingly consent or deny obscenity regulation, and regard indecency regulation as a violation of the First Amendment. Conversely, conservative religious groups and child advocates demand stronger restriction of the increased pornography on the Internet. The most fierce antagonism concerns the regulation of "indecent" or "harmful to minors" content on the Internet.

Apart from this normative debate over whether we

⁵⁰ <http://www.uiowa.edu/~cyberlaw/cls99/sempaper/baek416.html>

⁵¹ Prominent among these is the so-called Rimm study, published by Martin Rimm, a 30 year old researched at Carnegie-Mellon University who claimed that 85% of all images on the Internet were pornographic. While this paper and its findings have subsequently been widely critiqued in academic forums, it has nonetheless achieved a certain notoriety – not least because it was the foundation of a cover story in *Time* magazine.

⁵² A copy of the paper is included in the annexures to this report.

should restrain indecency or obscenity, when existing obscenity laws apply to the Internet, new conflicts occur in their applicability. As illustrated in Thomas,[90] community standards of the Miller test based on physical geographical jurisdiction do not appropriately operate in cases involving computer networks; computer networks create new concept of geography (or community) in cyberspace, which is not relevant to locations in the physical world. Potentially the most restrictive law in one jurisdiction could apply to the rest of jurisdictions in the nation. Pataki[91] also found that the geographical limitation of states' jurisdiction was meaningless on the Internet.

Two Congressional efforts[92] to impose access restrictions to protect children from exposure to indecent content were ruled unconstitutional due to broad definitions of "indecency" or "harmful to minors" speech and the unfeasibility of age-verification technology.

Civil liberty activism among absolute free speech groups suggests the print model as a regulatory framework for the Internet, opposing laws that regulate indecency.[93] Pornography regulation in the print model follows the principles of market competition and self-regulation which have long governed newspapers, magazines, and books.[94] However, courts have sustained states' restriction on "harmful to minors" speech and minors' access to "adult zones" such as adult bookstores and adult theaters.[95] Ginsberg was about print media in the physical world where it is possible to segregate indecent speech into certain areas to prevent minors' access. In this light, the print model is also restricted in terms of child protection along with self-regulation of markets. "Indecency" or "harmful to minors" speech is defined by community standards.

Emerging issues in the search for regulatory alternatives for the Internet are 1) new standards to determine obscenity in a new technological setting, and 2) feasibility of advanced technology to create constitutionally adequate cyber adult zones that prohibit minors' access and protect adults' indecent speech.

First, as Zanghi suggested[96] the "contemporary standards" of "society at large"-- without geographic limitations--could replace local community standards of the Miller test. According to Zanghi, the "contemporary standards" of "society at large," require an expert's statistical testimony based on empirical study of obscenity.

However, an empirical study is still problematic in determining obscenity like an effect study of pornography. Any single entity cannot produce the clear-cut definition of obscenity which will appease everyone in practice. To this end, public discussions and rational debates inside and outside courts will help to examine and develop new contemporary standards applicable to our new information age, as much as politics and other social institutions do. In fact, the Miller test was established in competition between different political forces to gain public supports, and local community standards have also been used based on public consensus through public discussion in the communities. In my view, the tension between absolute free speech advocates and child advocates will negotiate the scope of new "social (or national) obscenity standards" through public discussion and reaching a consensus. "Average person," applying new "social (or national) standards" would define the obscenity based on other two parts of the Miller test.

In cases involving obscenity coming from outside the U.S., an effective international regime would be an ideal solution. Currently, foreign commerce is also subject to 18 U.S.C. 1462;[97] a foreign distributor could be brought within U.S. jurisdiction. However, technological alternatives and negotiation between national sovereignties would be the second-best solution, as we have seen in international trade agreements.[98]

Second, zoning cyberspace would potentially realize the goal of protecting children without infringing on adults' constitutional rights, as Justice O'Conner already suggested in Reno I.[99] Zoning the Internet is analogous to real-space zoning found in adult book stores and theaters. This zoning concept, based on identity-verification technology, is not totally new and is already being applied to copyright protection.[100] "Indecency" or "harmful to minors" standards can be established the same way that obscenity standards

are established. In fact, the limitation of minors' access to "indecency" or "harmful to minors" content has long been held by states. Creating "locks" by advanced technology within the Internet, suggested by Sunstein, is also similar to the concept of zoning for constitutional regulation of indecency.[101]

The problem is that the zoning technologies are still expensive and burdensome on speakers, and are not available for all categories of the Internet like e-mail, mail exploder, and newsgroups. Like in Reno I, the court in Reno II[102] found that identification technology is still expensive for noncommercial and technologically unfeasible. Hence, Lessig's idea is that the more court cases dealing with current Internet conflicts, the better--until a zoning device is available.[103] The individual use of multiple rating and filtering systems will be useful as a voluntary zoning device.[104]

In conclusion, laws (whether old or new) require redefinition of standards, but traditional principles that protect minors from pornographic material generally stand firm. Current obscenity laws and the restriction of minors' access to sexually explicit content will effectively function with the establishment of new obscenity standards and the development of zoning technology. One last point is that courts need to consider the potential of the Internet as an open educational forum for young adults, as anti-censorship feminist groups argue. The applications of "harmful to minors" standards in courts will determine if the protection of children from pornography necessarily means the suppression of healthy discussion of human sexuality.

7.6.1 The concept of “adult” or “cyber-zoning” was also approved by the US Supreme Court in *Reno II*⁵³. Writing a separate opinion, partly concurring and partly dissenting, Justice Sandra Day O’Connor said⁵⁴:

“I write separately to explain why I view the Communications Decency Act of 1996 (CDA) as little more than an attempt by Congress to create “adult zones” on the Internet. Our precedent indicates that the creation of such zones can be constitutionally sound. Despite the soundness of its purpose, however, portions of the CDA are unconstitutional because they stray from the blueprint our prior cases have developed for constructing a “zoning law” that passes constitutional muster.

The creation of "adult zones" is by no means a novel concept. States have long denied minors access to certain establishments frequented by adults.⁵⁵(1) States have also denied minors access to speech deemed to be "harmful to minors."(2) The Court has previously sustained such zoning laws, but only if they respect the First Amendment rights of adults and minors. That is to say, a zoning law is valid if (i) it does not unduly restrict adult access to the material; and (ii) minors have no First Amendment right to read or view the banned material. As applied to the Internet as it exists in 1997, the "display" provision and some applications of the "indecent transmission" and "specific person" provisions fail to adhere to the first of these limiting principles by restricting adults' access to protected materials in certain circumstances.

⁵³ *ACLU v. Reno*, 521 U.S. 844, 138 L. Ed. 2d 874, 117 S. Ct. 2329 (1997). The nomenclature of the *Reno* cases is now somewhat confusing. There appear to be *four Reno* cases: (1) *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996), US District Court, commonly called “Reno I”, addressing CDA; (2) *ACLU v. Reno*, 521 U.S. 844, 138 L. Ed. 2d 874, 117 S. Ct. 2329 (1997), US Supreme Court, commonly called “Reno II” striking down the CDA as unconstitutional; (3) *ACLU v. Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999), US District Court, commonly called “Reno III”, addressing the constitutionality of the Children’s Online Privacy Act (“COPA”); and (4) *ACLU v Reno*, 2000 WL 801186 (3d Cir. Jun 22, 2000), affirming *Reno III*, and which we choose to call *Reno IV*.

⁵⁴ Justice O’Connor was of the view that the CDA was only *partially* invalid.

⁵⁵ A similar restriction in India restricts or prohibits minors’ access to movie theatres showing films with an ‘A’ rating, to liquor-vendors, bars, pubs, discotheques, etc.

Unlike the Court, however, I would invalidate the provisions only in those circumstances.

Our cases make clear that a "zoning" law is valid only if adults are still able to obtain the regulated speech. If they cannot, the law does more than simply keep children away from speech they have no right to obtain—it interferes with the rights of adults to obtain constitutionally protected speech and effectively "reduce[s] the adult population . . . to reading only what is fit for children." *Butler v. Michigan*, 352 U. S. 380, 383 (1957). The First Amendment does not tolerate such interference. See *id.*, at 383 (striking down a Michigan criminal law banning sale of books—to minors or adults—that contained words or pictures that "tende[d] to . . . corrup[t] the morals of youth"); *Sable Communications, supra* (invalidating federal law that made it a crime to transmit indecent, but nonobscene, commercial telephone messages to minors and adults); *Bolger v. Youngs Drug Products Corp.*, 463 U. S. 60, 74 (1983) (striking down a federal law prohibiting the mailing of unsolicited advertisements for contraceptives). If the law does not unduly restrict adults' access to constitutionally protected speech, however, it may be valid. In *Ginsberg v. New York*, 390 U. S. 629, 634 (1968), for example, the Court sustained a New York law that barred store owners from selling pornographic magazines to minors in part because adults could still buy those magazines.

The electronic world is fundamentally different. Because it is no more than the interconnection of electronic pathways, cyberspace allows speakers and listeners to mask their identities. Cyberspace undeniably reflects some form of geography; chat rooms and Web sites, for example, exist at fixed "locations" on the Internet. Since users can transmit and receive messages on the Internet without revealing anything about their identities or ages, see Lessig, *supra*, at 901, however, it is not currently possible to exclude persons from accessing certain messages on the basis of their identity.

Cyberspace differs from the physical world in another basic way: Cyberspace is malleable. Thus, it is possible to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws. This transformation of

cyberspace is already underway. Lessig, *supra*, at 888–889. *Id.*, at 887 (cyberspace "is moving . . . from a relatively unzoned place to a universe that is extraordinarily well zoned"). Internet speakers (users who post material on the Internet) have begun to zone cyberspace itself through the use of "gateway" technology. Such technology requires Internet users to enter information about themselves—perhaps an adult identification number or a credit card number—before they can access certain areas of cyberspace, 929 F. Supp. 824, 845 (ED Pa. 1996), much like a bouncer checks a person's driver's license before admitting him to a nightclub. Internet users who access information have not attempted to zone cyberspace itself, but have tried to limit their own power to access information in cyberspace, much as a parent controls what her children watch on television by installing a lock box. This user-based zoning is accomplished through the use of screening software (such as Cyber Patrol or SurfWatch) or browsers with screening capabilities, both of which search addresses and text for keywords that are associated with "adult" sites and, if the user wishes, blocks access to such sites. *Id.*, at 839–842. The Platform for Internet Content Selection (PICS) project is designed to facilitate user-based zoning by encouraging Internet speakers to rate the content of their speech using codes recognized by all screening programs. *Id.*, at 838–839.

Despite this progress, the transformation of cyberspace is not complete. Although gateway technology has been available on the World Wide Web for some time now, *id.*, at 845; *Shea v. Reno*, 930 F. Supp. 916, 933–934 (SDNY 1996), it is not available to *all* Web speakers, 929 F. Supp., at 845–846, and is just now becoming technologically feasible for chat rooms and USENET newsgroups, Brief for Federal Parties 37–38. Gateway technology is not ubiquitous in cyberspace, and because without it "there is no means of age verification," cyberspace still remains largely unzoned—and unzoneable. 929 F. Supp., at 846; *Shea, supra*, at 934. User-based zoning is also in its infancy. For it to be effective, (i) an agreed-upon code (or "tag") would have to exist; (ii) screening software or browsers with screening capabilities would have to be able to recognize the "tag"; and (iii) those programs would have to be widely available—and widely used—by Internet users. At present, none of these conditions is true.

Screening software "is not in wide use today" and "only a handful of browsers have screening capabilities." *Shea, supra*, at 945–946. There is, moreover, no agreed-upon "tag" for those programs to recognize. 929 F. Supp., at 848; *Shea, supra*, at 945.

- 7.7 Similar attempts at zoning in America have met with mixed success in court. In a case from Alexandria, Virginia, First Amendment concerns of free speech were cited before the U.S. District Court of the Eastern District of Virginia in *Mainstream Loudoun v. Board of Trustees*⁵⁶. The county library had chosen to institute a library system of filtering called 'X-Stop'. Like many filtering programs, X-Stop blocked some sites that do *not* contain objectionable material. The library board policy only permitted unblocking of a site against a written request to the librarian. This application had to contain the name of the site. The librarian then manually unblocked the site if the librarian was of the view that it fell within the scope of the library policy. The Library Board claimed that this was a reasonable restriction.
- 7.8 Commenting on this case in an article at Giglaw.com⁵⁷, Stan Morris says:

The judge ruled among other things that there were many ways to satisfy that purpose of keeping minors from accessing undesirable sites. These methods ranged from installing barriers making computer screens less visible to having a children's area where the computers were not connected to the Internet. Other choices were selective filtering such as putting filters on computers available in the children's area.

The court's ruling overturned the standard set by the library board. **The library's strictures would hypothetically block an English student seeking to research the works of D.H. Lawrence or John Cleland from using the Internet unless specifically granted permission by the librarian. Or, if unwilling**

⁵⁶ 2 F.Supp. 2d 783 (E.D. Va. 1998); 24 F.Supp. 2d 552 (E.D. Va. 1998)

⁵⁷ <http://www.giglaw.com/articles/2000/morris-2000-04.html>

to submit to the scrutiny of the public librarian, a scholar would be restricted to the level of a young child in attempting research.

(emphasis supplied)

7.9 *Kathleen R v Livermore*⁵⁸ was a case where the Plaintiff before the Court sought to restrain the disbursement of funds to public library computer operations so long as minors had access to materials ‘harmful to minors’. Morris says, about this case:

The court in this particular case, like the Virginia court, listed a number of less restrictive alternatives to library filtering **including filters only on terminals for children** or a system that would allow adults to turn off the filters. (emphasis supplied)

7.10 These two decisions and Morris’ commentary on them lend support to our recommendations that minors in Cyber Cafés be restricted to certain machines in an ‘open’ area, i.e., facing the common open space, and that these machines be fitted with filter software. They also provide judicial support to our rejection of proposals for site-blocking, across-the-board banning and monitoring.

7.11 Many commentators, jurists and Advocates, including Morris,⁵⁹ have commented on the duty of parents to supervise their minors’ use of the Internet. We do not quarrel with this proposition. Indeed, we support it fully. But we are conscious of the Indian context: frequently, children are better versed in Internet and computer technology than their parents; there is little concerted attempt to educate parents about potential

⁵⁸ Court Of Appeal Of The State Of California, First Appellate District, Division Four. The full text of the opinion is available online at <http://www.techlawjournal.com/courts/kathleenr/20010306op.asp>

⁵⁹ In *Livermore*, the Plaintiff was allowed to amend the case to argue that the library had a constitutional duty to supervise a minor’s use of the Internet. Morris’ view is that “Plainly, the city of Livermore must argue, correctly, that this duty falls on the parents and not on the library.”

hazards on the Internet, symptoms and solutions. Further, we are, for the present, focussed on Cyber Cafés which, as was pointed out in discussions, might be argued to be *in loco parentis* for minors who use Cyber Cafés unaccompanied by a parent. Our recommendations, therefore, strive for a balance between allowing – even encouraging – children to use the Internet, on the one hand, and ensuring that this use is safe, responsible and useful on the other. If a parent is not present at the time, then it falls to the Cyber Café operator to assume at least part of that parental role; and, as the foregoing extracts show, some of our recommendations are echoes of similar proposals already mooted in the west.

- 7.12 We also urge that our recommendations be seen as actually working *in the Cyber Café's interests*, not against them. Sooner or later, a major case will develop in which an unlicensed, unregulated and careless Cyber Café owner or operator will be rendered liable for harm caused to a minor. We believe that our recommendations are reasonable and, if followed, will safeguard the interests not only of minors but also of the Cyber Cafés who serve them. The same is also true of our recommendations for ISPs.

8 CONCLUSION

- 8.1 Under the guidance of the Chairperson, Mrs Tyagi, the Committee has thus attempted the demarcation, in a small way, of a child-friendly, or child-safe, 'Cyber Zone', one where minors could safely access and use the Internet for information, education, communication and entertainment. The Committee accepts that the Internet is not only the communication medium of the day but that is now virtually central to the full education of minors. There are many skills and technologies and much knowledge that only the Internet makes available so rapidly, easily and inexpensively. Children who lack these skills will, in the years ahead, be found wanting. The Committee accepts this view and sees it as a full-fledged rebuttal to the advocates of site blocking and banning.
- 8.2 Equally, the Committee accepts and acknowledges that its recommendations are neither comprehensive nor fool-proof. Indeed, they are not meant to be so. They attempt, as earlier stated, to create child-safe areas.
- 8.3 These recommendations are, thus, emphatically aligned *away* from blanket prohibitions. They are intended as a measures towards zoning, not banning.
-

SECTION 3 : RECOMMENDATIONS

1 CLASSIFICATION

- 1.1 Following the discussion on the issues categorised¹, the Committee has prepared separate recommendations for each category.
- 1.2 Within the regulatory category, separate recommendations are made for different classes of service providers, to the extent possible. Where possible or thought necessary, the Committee has attempted definitions and the preparation of *pro-forma* forms.

2 REGULATORY RECOMMENDATIONS FOR CYBER CAFÉS

2.1 Definition

The Committee approved the following definition of a Cyber Café and recommends appropriate statutory instruments to bring it into force

A Cyber Café means and includes any establishment by whatever name called, the object of the business of which is to make available to the general public, either for a fee or gratis or as part of rendering or supply of any other goods or services, access to and use of the Internet (in any of its forms or protocols, whether now in existence or yet to be implemented) for any purpose, including but not limited to, recreation and amusement, but does not include any place used purely as a residence or as an office or a place where access to the Internet is restricted to employees, staff or similarly authorised personnel; and a Cyber Café shall be deemed to be a place of

¹ Section 6

public amusement under Section 2(9) of the Bombay
Police Act, 1951

2.2 Licensing

The Committee approved a licensing application form required for Cyber Cafés. This *pro-forma* is an Annexure to this Report. The Committee recommends the adoption of this *pro-forma*.²

2.3 Personal Identification

2.3.1 The Committee recommends that every visitor to a Cyber Café be required to produce any photo-id card.

2.3.2 Regular users may be assigned membership and membership numbers free.

2.3.3 Children without photo id cards should be accompanied by an adult with a photo id card.

2.3.4 The Committee recommends that every licensed Cyber Café be required to maintain a physical log of users.

2.4 Physical Layout

2.4.1 The Committee recommends that all Cyber Cafés that have cubicles or partitions be required to ensure that minors are not allowed to use machines in cubicles or behind partitions.

² The form would be required to be filled in by existing Cyber Cafés also.

2.4.2 All 'open' machines must face 'outward', i.e., must be facing the common open space of the Cyber Café.

2.5 Software

2.5.1 The Committee recommends that all 'open' machines, to which minors are restricted, be equipped with suitable safety software.

2.6 IP Allocation /Access logs

2.6.1 Cyber Cafés who have a block of IP addresses from an ISP may choose to directly use them on their client machines. In such a case, they must maintain a list showing which IP address is allocated to which machine.

2.6.2 On the other hand Cyber Cafés with shared IP addresses (single or multiple), which are then shared amongst a number of local machine, must maintain an electronic log that shows the mapping of a unique physical IP with the 'masqueraded' IP. The actual method used is irrelevant, so long as the Cyber Café is able to tell the authorities, on demand, during enquiry, which machine was allocated which IP address at a specified time.

2.6.3 It is clarified that these logs must not be of every activity carried out at the terminal, but only of the IP address allotted by the Cyber Café server. These logs are to be maintained for at least three months.

3 REGULATORY RECOMMENDATIONS FOR ISPs

3.1 Email

3.1.1 USING LOCAL CLIENTS

- (a) Accurate time stamps must be incorporated by the outward SMTP server. The time should be synchronised with the local ISP in order to maintain coherence.
- (b) Also the entitlement of the customer must be ensured; all ISPs must deny relaying. For example xyz@vsnl.com customer should not be able to send mails from rediffmail.com's smtp server.

3.1.2 USING THIRD PARTY SERVICES (TPSS)

- (a) As the authentication of identity cannot be ensured in a third party free web-based service, proper logs with time stamps should be maintained and forwarded immediately to investigating agency in case of enquiry.

3.2 Connectivity and Authentication: ISP Level

- 3.2.1 All the dialup customers should have non-repudiatable authentication and usage records.
- 3.2.2 The Remote Access Servers should have the some form of Caller Identification feature set up so as to log the telephone number from where the connection was established³.

³ For this coordination with the BSNL authorities is essential as in many cases the ISP's end equipment has the feature, but the main connectivity provider (BSNL) does not have the feature or is not enabled.

3.2.3 All Remote Access Dial In User Service/Server (RADIUS) logs should be saved on some reliable removable media for permanent storage and easy retrieval⁴. It may be stored in a universal zipped format in order to conserve space and recorded on a monthly basis.

3.3 Time clock coordination

3.3.1 All time clocks on ISP systems must be regularly checked and synchronized with universally accepted time synchronization services such as the Cesium Atomic Clock.

3.4 Record Keeping

3.4.1 As part of the terms of licensing of every ISP⁵, every ISP should be required to include on all application forms for an Internet connection information as to whether the connection is being taken for use in a Cyber Café.

3.4.2 If so, further information, sufficient to ascertain the Cyber Cafés control systems, should be separately taken by the ISP and kept on file.

⁴ Such as Compact Disks, etc

⁵ ISPs are licensed by DOT

4 EDUCATIONAL MEASURES

4.1 Email newsletters

4.1.1 The Committee recommends that every ISP be required to send out periodic email newsletters to all subscribers (not just Cyber Cafés). This newsletter *must* contain information and warnings directed to parents about the ill effects of cyber pornography on minors and possible remedial measures.

4.2 Online information

4.2.1 Similarly, the ISPs portal pages online must include information and warnings directed to parents about the ill effects of cyber pornography on minors and possible remedial measures. This is, typically, visualized as being more detailed than the information contained in the newsletter.

4.3 Protective software

4.3.1 The Committee recommends that every ISP be *required* to offer its subscribers protective software, either for online download or on the Compact Discs containing the dial up connection installable and executable files.

4.3.2 The software may be offered free, or at a price in Indian rupees, or combined with some Internet connection package. Users have the option of taking the software.

4.3.3 The Cyber Crime Investigation Cell of the Bombay Police shall establish a telephone hotline to address the needs of parents who find that their minors are being victimized by cyber

pornographers, stalkers, etc. The services would include counselling and therapy from specialists at a hospital and at the Tata Institute for Social Sciences, with which the Social Services Branch of the Mumbai Police already has a tie-up. Investigation and detection procedures would be followed up by the CCIC.

4.3.4 The hotline telephone number will be made available to the public on the CCIC website and every ISP will be required to publish it on their online portals and, optionally, in their email newsletters.

4.3.5 The Internet Service Providers Association of India and the CCIC must co-ordinate among themselves and with experts in Internet technology and social sciences, to conduct online and offline camps and seminars, including at school and college levels, to educate the public about the adverse effects of cyber pornography on children, protective and remedial measures and detection mechanisms. These camps must be scheduled on a regular basis.

**Mrs Archana
Tyagi**
DCP
Enforcement
Chairperson

Dr Sourav Dutta
VSNL

Mr Vijay Mukhi
IUAI

Mr Shashi
Kumar Nair
Advocate

Mr Gautam Patel
Advocate