

自由當自決 自助助人助之

*Freedom of Choice,
Participation and Mutual Help*

Response to COIAO Public Consultation

- Chapter 4, Paragraph 2.4

**Proposed Solution Jointly Prepared
by HKISPA and HKCSS-ITRC**

Submitted by: Hong Kong Internet Service Provider Association

Date: 30 January 2009

Table of Contents

I	Executive Summary3
II	Contact Information4
III	Solution Summary5
IV	Design Principle6
V	Current Situation7
VI	Goals and Objectives9
VII	Technical Component10
VII	Non-Technical Components13
IX	Evaluation Plan17
X	Future Development Plan18
XI	Estimated Timeline19

I. Executive Summary

Hong Kong Internet Service Provider Association (HKISPA) and Information Technology Resource Centre (ITRC) of The Hong Kong Council of Social Service (HKCSS) jointly propose a solution, named “Parents’ Concerns on Internet” (PCI), as a response to the COIAO Public Consultation Chapter 4, paragraph 2.4 – discussion on mandatory provision of server side web filtering service by ISP.

Parents in Hong Kong are now facing serious challenges in protecting children from inappropriate content on cyberspace. While it is important to safeguard free information flow and help children to enhance their information literacy, parents still look at ‘filtering’ as one of the major means to ensure proper use of Internet at home.

However, there is no well-defined blacklist that suits the local context for parents to make reference to. And some parents, especially those less educated ones, are lacking the necessary computer knowledge to adopt such a blacklist even there were one available.

The mission and purpose of this solution is to enable parents to have freedom of choice in selecting various levels of protection for their children in the cyberspace. A community blacklist will be established, managed and used by parents to protect their children through the help of community assessors.

This proposed solution consists of three components. They are namely the technical infrastructure; the community blacklist; and the filtering support service. The technical infrastructure for the solution is proposed by HKISPA and the last two components were mainly contributed by HKCSS.

HKISPA is very familiar with ISP operations. Its input would ensure feasibility of the proposed technical solution. The HKCSS has a strong network of NGOs which would be leveraged to fuel the momentum required for engaging and supporting parents, together with the input from the parents-teachers association in all districts within the territory. It is believed that the cooperation will generate the kind of synergy needed for creating a safe environment for youngsters in Hong Kong.

II. Contact Information

Hong Kong Internet Service Provider Association

1803,
Chinachem Exchange Square
1 Hoi Wan Street,
Quarry Bay,
Hong Kong

Primary Contact

York Mok
Chairman

Tel: 2114-0067

Email: york@hkispa.org.hk

Secondary Contact

Ben Li
Secretary

Tel: 2114-0067

Email: ben@hkispa.org.hk

The Information Technology Resource Centre Limited

11/F.,
Duke of Windsor Social Service
Bldg.,
15 Hennessy Road,
Wanchai,
Hong Kong

Primary Contact

Tony Lee
Chief Development Officer

Tel: 2876-2420

Email: tony.lee@hkcss.org.hk

Secondary Contact

Richard Chow
Project Manager

Tel: 2876-2413

Email: richard.chow@hkcss.org.hk

III. Solution Summary

The purpose of the “Parents’ Concerns on Internet” is to empower parents in protecting their own children from inappropriate content in the cyberspace and allows freedom of choice at the same time.

Such empowerment would be achieved in 4 main directions.

1. Incubating a parents association in maintaining a “community blacklist” for filtering inappropriate website.
2. Promoting the adoption of the blacklist amongst filtering software vendors, ISPs, families and individuals and advocating active participation of parents and the community at large.
3. Allow maximum flexibility of subscribe and unsubscribe from blacklists of well defined subject or contributed by various organizations.
4. Supporting needy families to install and setup filtering solutions under the sub-programme “Filtering Support Service”. And ensuring that those households, especially families with children, that would like to have filtering system installed on their computers, would have access to one.

The proposed components are not only able to provide parents with a blacklist that suit the needs of those who wanted it, but also open up an opportunity for parents to overcome the technical barriers in implementing the filtering system.

IV. Design Principle

The proposed solution was designed based on the following principles:

- *Freedom of Choice (自由當自決)* – we believe that internet users should be able to decide for themselves what information to receive; whether their computers should be installed with filtering software; and what filtering software to use. As would be indicated in the following sessions, websites on the blacklist would be classified into levels of obscenity. Users could select according to their own choice the level of filtering to adopt. Moreover, the blacklist is supposed to be released to other security software companies so that users could have a choice of using other software application while referring to our community blacklist, should the filtering application developed in this solution be seen as inappropriate for some users.
- *Parents' determination (自助人助之)* – We acknowledge the rights and duties of parents to construct an environment which they see as suitable for their children to access internet at home. We look at that as a crucial part of parenting in Hong Kong nowadays. Although that should be the ultimate responsibility of individual families to determine to what extent decisions should be made for their children under 18, we also believe that it is necessary to provide help to families with specific needs, for example to those parents who realise they need to exercise tighter control for their kids in accessing the internet and yet are in lack of the technology to do so. We believe that such need might be greater in families with disadvantaged kids or parents. This solution is empowering in nature because it provides such families with one more easy-to-use technical option.
- *Freedom of Speech* – As a result of the second phase of the World Summit on the Information Society, the Tunis Agenda for Information Society was endorsed by many countries including China.

The Agenda reiterated that the international community has a '... commitment to the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge. and that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.'

The current solution aims at balancing the expectation of parents to filter inappropriate materials while ensuring that those parents who defy filtering would not be affected.

V. Current Situation

Parents in Hong Kong are now facing serious challenges in protecting their own children from inappropriate content on cyberspace.

A. The need for a community blacklist

There is a large group of parents who want to opt for a clean Internet environment for their children in Hong Kong. The best way to do it is control from the source. At the moment, the legislation Cap 390 alone, although implies an intention along the same line, when the publisher of the websites with obscene content is outside Hong Kong it has been ineffective in doing so.

Filtering then becomes the other option for parents. Nevertheless the effectiveness in blocking inappropriate web content is highly dependent on the blacklist that a particular filtering solution refers to.

Since most of the filtering solutions in the market refer to a blacklist that target English contents, they may not be sufficient to tackle the local problems. Since much of the inappropriate content is in Chinese, blacklists compiled overseas would definitely be insufficient in filtering such content.

In addition, blacklists referred by these filtering solutions are usually created and maintained by an authorized agency, government departments of foreign countries, or even by the filtering software vendor itself. The channels for users, including parents, to report any suspected inappropriate websites is very limited. We trust there is a group of frustrating parents who, although had installed some kind of filtering applications, do not find the existing application capable of doing the job effectively. That is because of two reasons:

- 1) the lack of easy-to-use functions to add to the blacklist the application refers to;
- 2) the lack of time and personal capacity to tackle the speedily growing volume of inappropriate content.

The community blacklist proposed in this solution is one that comes from and belongs to the community. It allows a concerted effort of all parents involved and the community at large too to report indecent content, determine the level of decency collectively and objectively, and adopting it automatically, while leaving individual parents to determine the level of filtering used in their families. Assessment of the websites would be done online, by random assignment of assessors. Web 2.0 methodology such as credibility checking would be adopted to reduce the chances of malicious use of the reporting mechanism.

B. The need for a technical support service

A “Promoting the Use of Filtering Software” programme was organised by The Television and Entertainment Licensing Authority earlier this year to provide financial supports to schools and non-governmental organisations to conduct talks or workshops to teach parents about the need and procedures for installing filtering software. There is a plan to further strengthen the programme by providing shortlisted filtering software free-of-charge. But even such help would not guarantee success due to the low ICT skill level of some parents.

Similar initiatives had been launched in other countries and failed.

The Australian Government had initiated the “National Filter Scheme” in year 2007, in which over AUD 85 million (~HKD 612 million) was spent to provide every Australian household a free client-side filtering software. The scheme also came along with undertaking awareness raising campaigns and activities in schools.

Expected usage of the software was 2.5 million households, yet after 12 months, only 144,000 filtering products have been actually downloaded or ordered on CD-ROM and only about 29,000 (20%) of these products were still being used. Despite over AUD 15 million being spent in advertising to support the scheme, the programme had clearly failed.

It is obvious that a wider adoption of filtering products in families, and by parents, would require more than a list of free filtering software, download links and awareness raising campaigns. The parents shall also be supported to overcome the technical barriers of installing and configuring the products. Moreover, education and support to parents should also cover the importance of information literacy at the same time, emphasizing that ‘filtering’ alone is not adequate for the growth and development of children.

In summary, there is no well-defined blacklist that suits the local context for parents to contribute and make reference to. Also, parents are lacking the necessary computer knowledge to adopt such a blacklist even there was one available.

VI. Goals & Objectives

The ultimate mission of the proposed solution is to empower parents in protecting their own children. The mission could be achieved by following goals and objectives.

1. Incubating a parents-maintained “community blacklist” of inappropriate website.
 - a. To establish a parents’ association with the help of supporting organisations.
 - b. To train a group of assessors consists of parents and invited members from the community.
 - c. To technically setup and maintain a local blacklist.

2. Promoting the adoption of the blacklist amongst filtering software vendors, ISPs, families and individuals and advocating active participation of parents and the community at large
 - a. To develop an independent filtering service infrastructure.
 - b. To engage filtering solution providers in adopting the blacklist.
 - c. To provide a channel for parents and the community at large to report inappropriate websites.
 - d. To provide a free-of-charge filtering solution.

3. Supporting needy families to install and setup filtering solutions under the sub-programme “Filtering Support Service”. And ensuring that those households, especially families with children, that would like to have filtering system installed on their computers, would have access to one
 - a. To train up a group of youth as helpers to facilitate the need.
 - b. To promote the use of filtering solution and encourage adoption of the blacklist.
 - c. To provide a hotline service for basic technical support on filtering solution and blacklist.
 - d. To provide a free-of-charge filtering solution installation and configuration service.

VII. Technical Component

The technical solution is prepared by the HKISPA in due consideration of feasible technical options and social impact.

A. Issues to be Addressed

i. Server Side Filtering

Server Side Filtering solutions based on user login name (Login ID) as the identifier. When user initiates an Internet connection, system will redirect the upcoming web traffic to filtering devices if the Login ID has the filtering service associated. However, not all HK ISP require user login, access is automatically granted base on the physical circuit termination location. Without client side software, such households are limited to single profile. Similar situation happens in home Wi-Fi environment where login ID is normally set in the broadband router. Modifying the setting requires networking knowledge and there is only one active profile running. i.e. all web traffic, from parents or children, are treated equally at any one time.

ii. Adaptability of Filter Lists

Filter list maintainers making decisions base on their local culture and standard. None of the current popular filter list is designed and maintained in Hong Kong. Also, no single filter list fits all. Users require lists from wide range of subjects and confidence levels to suit their individual need.

iii. Social Concerns

There are two major concerns from the society:

1. Mandatory web filtering mechanism will be utilized to control freedom of Internet usage in Hong Kong.
2. Most parents are less technically competent than their children. The web filtering protection could be bypassed without notice.

B. Proposed Technical Infrastructure

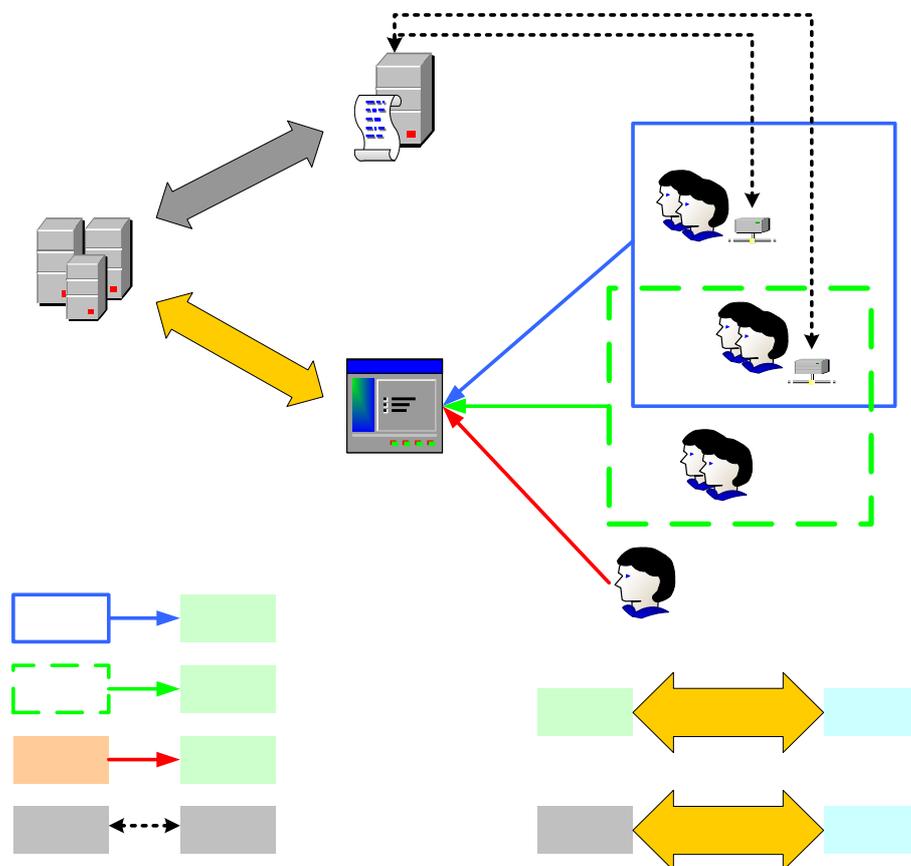
i. Objectives

In order to develop a web filtering system which can address the needs of Hong Kong Internet users, our proposed solution should:

1. Perform filter action on the client side, so that users have full control on installing the program or not.
2. Support multiple user profiles on a single machine.
3. Code the client side program under Open Source framework to eliminate hidden actions.
4. Allow users to decide the most suitable protection by subscribe to filter lists with different targeted subjects and severity levels.
5. Allow users reported harmful contents to be added into filter list. Assessor system to maintain balanced view for reported contents and construct multiple levels of lists.
6. Provide mechanism for listed URL owners to raise objection.
7. Be extendible to wider service scopes.
8. Have no impact to current ISP infrastructure.

ii. System Code Name: FiLial2.0

FiLial is the short form of Filter List ally: filter lists platform for various purposes and confidence levels are allied together. Web2.0 means user generated contents; FiLial2.0 supports user contributed and maintained filter lists.



High Level Diagram of FiLial2.0

iii. FiLial2.0 Building Blocks

There are four major components of FiLial2.0.

1. The Portal: front end for all human activities:
 - User account management
 - Filter list selection
 - Report harmful content URL
 - Rate reported URLs by Assessors group
 - Verify presents of a URL on lists
 - Raise objection from URL owner
 - View user reports
 - Get supporting information
 - Portal for recommended contents e.g. web sites, news groups, forums, Blogs
2. The Upholder: maintain all machine-to-machine activities:
 - Dispatch latest black lists to users machine
 - Record user status changes information
 - Synchronize black lists to/from third parties
3. The Backend: data repository and where batch job runs:
 - Database for the whole system
 - Generate various reports
4. The Client: a simple client side program which performs the filtering according to operation mode and black lists subscribed:
 - Synchronize subscribed black lists from The Upholder
 - Report user status changes to The Upholder
 - Allow user switching from profiles
 - Under “Protection” mode, user require password to turn off web filtering
 - Under “Harmony” mode, this is design for teenage children. No password is required to turn off web filtering
 - All status changes in both Protection and Harmony modes will be recorded and shown in user report

VIII. Non-Technical Components

A. “Parents’ Concerns on Internet” - community blacklist

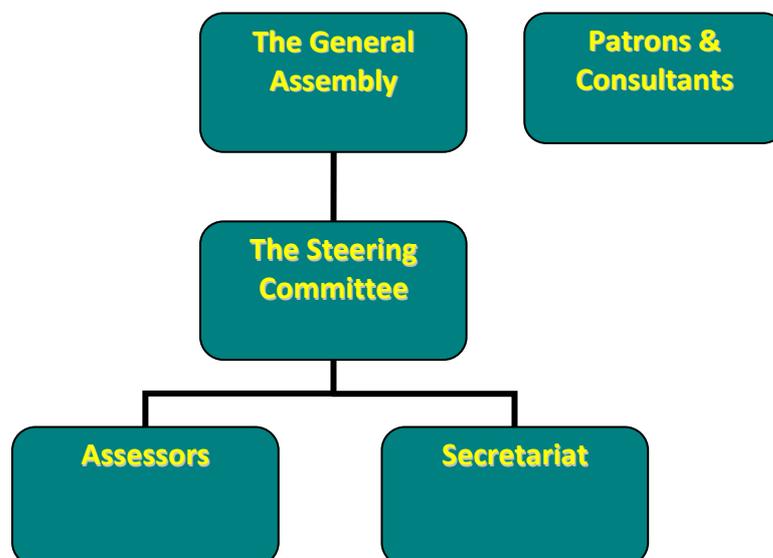
The major task is to set-up a structure to assess reported web materials, to manage the community blacklist and to facilitate related operations. We have a plan to engage the Federation of Parent-Teacher Associations in all districts of Hong Kong via the network and help of the Committee on Home-School Co-operation. Initial exploration has led us to believe that the motivation of the Federation should be quite high in mobilizing more parents to participate in the program. Parents can participate in various ways as illustrated in the diagram below.

The General Assembly consists of parents who are users of the filtering list. By joining the PCI assembly they are entrusting the assessors to determine the level of decency of each reported website. The assembly appointed people to serve at the steering committee which controls the operation of the Secretariat and the assessors group.

At the beginning, HKCSS may play the role of the Secretariat and provide assistance for the General Assembly to establish itself, with the help and advice from the Patrons and Consultants group.

Meanwhile, this solution has also noted a support from SchoolNet, a company that is currently providing filtering service to schools. SchoolNet will provide on a pro-bono basis their blacklist for the PCI to kick start. Therefore parents joining the program could expect the same list operating at both school and home environment.

The PCI’s organization chart.



The Patrons and Consultants will be formed by members of the Hong Kong community who can

- provide the kind of legitimacy that PCI needs in its conception and development;
- provide the experience and expertise required by PCI

The General Assembly is the big parents group which all parents in Hong Kong could be part of. It is the basis of the whole structure. By choosing to use the filtering softwares that refer to the “blacklist”, parents become members to the PCI general assembly and delegate the authority to the PCI Assessors to categorize websites for them.

The Steering Committee will provide overall direction and consist of

- active parents in the general assembly;
- community leaders invited by HKCSS;
- representatives of funders.

The Assessors group consists of parents and invited members from the community who would be trained to provide the assessment for the reported online materials. To maintain consistency for the assessment, a set of criteria will be developed and assessors would be trained and supported by agency members of the HKCSS.

The Secretariat of the structure will be taken by HKCSS, which

- facilitates the concerned workflows of PCI particularly in website assessment;
- facilitates the establishment of PCI as an independent, sustainable NGO;
- maintains the membership database of PCI;
- maintains the “blacklist” and its utilization on behalf of PCI.

Function of the PCI

After setting up the aforementioned structure, the PCI will facilitate the following tasks:

- To establish and maintain the blacklist that is suitable for local context;
- To engage parents' and communities' input in reporting inappropriate contents;
- To establish a mechanism of listing or delisting a reported webpage by constructing a set of assessment criteria in classifying inappropriate contents;
- To organize the blacklist and liaise with filtering vendors in adoption of the list;
- To promote activities in parents' community and encourage both reporting and usage of filtering solutions to protect their children online;
- To collaborate with NGOs and other professional bodies to promote protective and preventive measures against online and ICT risks among parents.

B. Filtering Support Service

The Goal of this solution is to support needy families to install and setup filtering solutions. A support team will operate with the support of The Hong Kong Council of Social Service network which consists of over 350 member agencies (NGOs) with over 3,000 service units throughout the territory.

The team aims to provide on-site support in installation and configuration of filtering solutions to parents who have no or limited computer knowledge throughout Hong Kong.

Computer centres currently operating by NGOs in the community will also be leveraged. The support team would either be anchored to these current sites, or be hired from the support staffs of these sites. In this case, we could make best use of the ICT capability and the human resources of these NGOs. A fast response to request from community users can also be expected.

To help the parents in trouble-shooting of the filtering solutions, a hotline will also be set up to provide helpdesk support service for users' inquiry. Besides inquiry, parents could also order for an on-site support service free-of-charge. But families that can afford to pay for the service, a reasonable and very limited amount of donation (\$50-100 per order) would be suggested to cover part of the cost of operation. The donation would be purely voluntary in nature.

At the moment, the plan is to have a few capable NGOs selected to manage the group of technical persons who are willing to conduct the field work in the community. Apparently, according to our knowledge at this moment, NGOs are interested in recruiting unemployed but capable youth to contribute to the solution. An honorarium will be provided for each on-site support conducted. PCI would also make use of such rare chances of on-site support for parent education, both in the use of the filtering application and in the general mindset of parenting in information age. The parenting training materials would be developed by experienced social workers. Should other special needs be detected during the on-site support, appropriate referrals would be made to social service organisation for follow up work.

IX. Evaluation Plan

The evaluation will be approached from inside, focused on the adoption numbers of the blacklist and filtering solution.

At the end of the second year after the establishment of PCI, we want to see the following outcomes and outputs:

- Establishment of a growing community blacklist maintained by parents
- A group of 1,000+ active trained assessors can be maintained
- Successful development of a free-of-charge filtering solution
- 40,000 families adopt the community blacklist
- 20,000 families used the filtering support service

X. Future Development Plan

Since the technical solution proposed by HKISPA - FiLial2.0 is a list management platform which supports user generated and rated black, and probably white, URL lists. As the platform and operation mature, it may consider expanding the service into other areas, for example:

- School, Library, Government Wi-Fi where mandatory client side program installation is not feasible. Gateway based solution could be considered.
- Illegal software download, obtaining P2P seed files, social network web activities, leisure online contents which are less preferred in working environments. Companies may also deploy similar filters on their Internet gateways.

XI. Estimated Timeline

Time (working days)	PCI and Secretariat	Organization & System Development	Hardware & Infrastructure
Day 0	Preparation of PCI establishment	Secure of Funding	
Day 20		Technical Committee form – kick off functional requirement	
Day 40	Establishment of PCI secretariat	Issue programmer tender	
Day 55		Tender reply	
Day 60		Technical staffs onboard	
Day 70	Set-up of assessment criteria		Development environment requirements finalized
Day 80		Tender award	
Day 90	Promotion to community Recruitment of assessors	Functional design finalized, coding start	Development environment ready
Day 105			Finalize infrastructure design, start tender preparation
Day 130			Issue hardware and infrastructure tender
Day 145	Briefing sessions to relevant organisations		Tender reply
Day 155			Tender award
Day 180	Liaison with filtering software vendors	Modular tests start	
Day 200	Training of Assessors		Infrastructure ready
Day 210	Set-up of hotline service	Trial from selected group	
Day 240	Roll-out of reporting system and assessment mechanism Delivery of installation and support service	Service launch	
Day 300	PCI register and incorporate as a NGO		
Day 300 +	Maintenance of blacklist Public education & awareness campaign		