Web and Content Filtering in Pakistan

Report 2011

7/8/2011

Pakistan Telecommunication Authority

1. Mechanism for content filtering over internet in Pakistan:

1.1. Background:

The Prime Minister of Pakistan in 2006 has formed an Inter-Ministerial Committee. The backdrop to the formation of this Committee was to take care of any unwanted/offensive content on the internet viewed in Pakistan. The Committee decides blocking of the websites to preserve and safeguard National Security and harmony.

The committee is headed by Secretary Information Technology and the members are from Ministry of Information & Broadcasting, Ministry of Interior, Ministry of IT, Cabinet Division and agencies.

The Inter-Ministerial Committee in its 17th meeting dated 29th September, 2010 constituted a Sub-Committee. The mandate of the sub-committee is to devise the effective mechanisms for Internet Content Filtering on national level.PTA is made the convener of the sub-committee whereas the other members are the representatives from Ministry of IT, PTCL, and agencies.

1.2. Approach:

The Sub-Committee held its 1st meeting on 25th October, 2010 in PTA after the release of the ToR by MoIT on October 7, 2010, to discuss the agenda and the roadmap. In the consequent meetings, the sub-committee met and had detailed discussions with the Etisalat representative Mr Haj Mahmoud who shared his UAE experiences from another perspective that is, UAE a country with limited de-regulation, and limited ISPs and Service providers. The sub-committee invited multiple Tier-1vendors in the field of content filtering, in order to obtain the technical know-how of the latest solutions and features available in the world.

The following sections of the paper discuss point by point the items of the Terms of Reference issued by MoIT (attached as Annex A), in light of the latest filtering solutions available and recent world wide practices.

1.3. Analyze international best practices for blocking pornographic / anti state content over internet and role of ISPs/Operators worldwide

1.3.1. International Practices

Blocking of undesired websites is normally done through filtering techniques. It is found that censorship of the Internet is commonplace in many regions of the world. In most countries , since

2002-2003, there has been an acceleration of efforts to either close down or inhibit the unwanted content on the Internet. In some countries, for example in China, Iran, Saudi Arabia, & Singapore etc, the level of monitoring and censorship is such, that the Internet is relatively quite prohibitive for users. While some states, such as Cuba, severely limit Internet and e-mail access.

According to the Open Net Initiative (ONI), an academic consortium that has been following global Internet filtering since 2002, more than forty countries now practice Internet filtering to some extent at the national level.

Some countries like USA, China, Iran and India have developed indigenous solutions for web filtering. Iran initially implemented Western filtering technologies but now it has developed an extensive and sophisticated indigenous solution and strictly regulates the web content. Due to the increasing role of internet in influencing the political, social, cultural and religious values by external elements, an indigenous solution is preferred.

The general trend of the deployment hierarchy of the filtering solution, being observed in most of the countries is, to deploy a system at international gateways, with few specific guidelines to ISPs*. Countries and proactive service providers normally formulate a policy based on categorization of their content and perform filtering for either national goals or for commercial purposes.

There is no one universal model for Internet content regulation. Each country's regulation of the Internet is driven not by technology or law but by the culture and society. Each country has its own specific concerns and hence the web content is handled and regulated accordingly.

Few countries like china regulates the web content on ***white list philosophy*** i.e. all the content on the web is black except a few which Government allows to enter its country. And few countries like Saudi Arab, Iran, Bahrain etc follows ***black list philosophy***, i.e. all the content on the web is white / allowed except a list of few which the Government blacklists and hence doesn't allow to enter the country. A few countries like Iran and Saudi Arab impose heavy penalties on ISPs for violating the rules of filtering.

As of today, Saudi Arabia, UAE, Kuwait, Bahrain, and Oman use SmartFilter technology to block content across content categories such as websites that provide critical views of Islam, secular and atheist discourse, and adult sites, they even block proxy and anonymity tools. Iran once used the western smartfilters technology but now it has developed its indigenous solution.

Tunisia also blocked content in these categories until January 2011, when an uprising led to diminishment of the country's filtering regime. Other countries such as Libya, Morocco, and Jordan also implemented Internet censorship to various degrees.

1.3.2. Role of ISPs/Operators worldwide

URL filtering technologies are used in many countries by their respective ISPs due to regulatory requirements, political mandates and marketing offerings. In Kingdom of Saudi Arabia there are reported to be fewer than 10 ISPs, of which probably 3 to 4 are big ones. In UAE there are only 2 ISPs. Countries with fewer ISP licenses (comparable to landing station or major carrier licenses), have a more rigorous filtering policy. However China is an exception with thousand or more ISPs and which has one of the most rigorous policies and important decisions are taken to stop pilferage of information which may dent their political stability.

In the West, ISPs offer URL filtering as a paid service to enterprises (employee productivity) and end users (parents). In some other countries ISPs/operators provide filtered content of various categories on commercial basis to increase their subscription, as value added service

Please refer to Annex B for country specific international Practices.

1.4. Analyze effectiveness of mass level technical filtering, its limitations and repercussions of censorship and propose mechanism in the light of the current capabilities.

Mass level filtering is preferred in countries with huge web users, numerous ISPs and a few entry-leave data points (satellite communication not considered) in a country. Available techniques with associated caches make them very attractive and also feasible for operators. An effective blacklist without using wildcards with an associated white list in the adopted technical solution is advisable.

1.4.1. Effectiveness/Efficiency of Mass Level Technical Filtering:

The effectiveness of a mass level filtering solution is governed by many of the following attributes:

1. **Size and Performance:** The solution addresses the current and future Internet traffic demands. The capacity, scalability and performance of the system should be such that meets the current and the future demands of internet traffic.

2. **Deployment Scenario:** The solution deployment configuration impacts traffic coverage, performance and cost.

3. **Filtering Accuracy**: The filtering accuracy includes the filtering based on URL, IP Address, Proxies, Protocols and virus filtering all in one solution. The solution programming,

performance and database comprehensiveness, balance between false positive and fals negative errors also dictate the accuracy of filtering URLs.

4. **Database(DB) Comprehensiveness**: A solution that has detailed and well defined categories and sub-categories in the DB. The DB must be reliable, up-to-date and also updated periodically, offers flexibility and performance gains, accessible and modifiable by the implementer dictates the comprehensiveness of DB.

5. **External Attacks Handling**: The system should be fool proof, should handle DDOS, virus or any other attack to bug it.

6. **Standardize & Modular solution:** Integrating the solution with other technologies effects its deployment, policy configuration, performance and cost. All measures should be taken to ensure a low cost solution which can be easily adapted to environment and minimum Intellectual Property rights.

7. **Vendor Support:** This is a major factor that makes or breaks the solution effectiveness. 24/7/365 local support is a must to effectively address traffic demands and technical faults. Local R&D also plays a very important role.

1.4.2. Limitations and Repercussions of Censorship

There are several major Limitations & repercussions of censorship i.e. political, social, religious and cultural etc. Setting the limitations is most curtail and difficult task and its definitions may change from person to person and over time.

Settings of the limits should be done by 'standardization committee' which should comprise of major stakeholders and approved by the GoP. However until such limits are being developed, a simple but capable system should be in place in ninety days.

1. Limitations:

a. Potential Legal Problems –

There are no meaningful external/ international limitations on a country's ability to filter the Internet access of its citizens, except WSIS and WTO. If certain websites are blocked in violation of the constitution then,

i. The individual or corporate owners of those blocked websites may approach judiciary for relief.

ii. Tools such as trade agreements and diplomatic pressure can convince states to alter their filtering behavior and its policies on cyberspace freedom.

b. Standardization of censorship –

This is a real difficult step in the mechanism of filtering to standardize and define which content to filter and which to let go, keeping in view all the social, legal and religious point of views on board. Therefore it should be defined carefully on broader spectrum, respecting the views of all major stakeholders

Even there is wide disagreement observed worldwide, as to what content should be accessible to citizens. The definition of "indecent" material in the United States would let pass material that would be deemed off-limits in much of Europe, and certainly in countries like Saudi Arabia or other parts of the Middle East. Various national views on "indecency" reveals the enormous complexity of formulating an international standard. Hence it seems unlikely that any single standard could serve as an international model.

Therefore there is a need for a strong national policy/ framework to be formulated in the light of the constitution, that clearly reads the definitions of the content to be blocked in a country.

Clearly specify the limits to which the political content, indecent content, anti state and national security related content, human rights violating content, religious, sect discriminating content etc. should be blocked.

Above all, in order to avoid any undesired reaction from any citizen or working body, the framework should also state which parameters would be used to evaluate the controversial religious and political content, in case the block request is generated.

Filtering does not protect against cyber-terrorism to extent, as the emails and peer-to peer communication, instant messaging and file sharing protocols are not filtered unless deep packet mechanisms are applied.

c. Technical limitations of Censorship –

i. **Over Blocking** – Also called false positive error blocks the permissible and authorized websites and content. This leads to users annoyance and dissatisfaction. Countries following blacklist philosophy often face this problem at a large scale.

   a) When an IP address is blocked, there is a significant chance that many unrelated Web sites will be blocked in the process. When an IP address is blocked, all sites virtually hosted on that server will be blocked. ("virtual hosting," a term that refers to the way in which many thousands of individual Web sites can be hosted on a server at a single IP address.)

ii. **Under Blocking** - Also called as false negative error allows inappropriate websites to pass through the filter reducing its efficiency.

iii. **Periodic Update:** Information on the Internet changes in a rapid and continuous manner forcing the filters to update at the same rate. A highly accurate filter may thus prove to be inefficient if it does not update itself with this change.

iv. **Balanced filter** that neither produces false positive not false negative errors does not exist, and thus a balance between the two filtering errors is highly desired.

2. Repercussions :

a. Domestic Political/ Social/ Religious/ cultural repercussions

Non conformity of definitions due to varying interest groups.

b. International Political/ Social/ Religious/ cultural repercussions

International norms and enforcing domestic policies on other countries.

1.4.3. Proposed mechanism in the light of the current capabilities.

1. Current Capabilities of Pakistan content blocking:

Currently there is no effective mass level filtering mechanism. The blocking capability is small fraction of the total Bandwidth. Due to phenomenal growth in internet traffic and limited capability of blocking, operators find it very hectic and difficult to block the bulk sites manually, involving extensive amount of iterations and reworking.

The web blocking technology Worldwide has matured many folds and many tools and solutions are available to electronically scan and filter as many as 100,000 URL requests and blocking more than 100 different categories, through IP address blocking. URL blocking, Composite blocking, Protocol based blocking and many other.

A mass level faltering mechanism located centrally at the traffic entry/exit points is proposed for our country. Incorporation of the caches may be operator's option. The ISPs shall ensure that they either stop using other means of acquiring international bandwidth or cache, otherwise block all sites (URL, IPs etc.) categorized by the central system.

2. Proposed Filtering model

The filtering regime should embrace three prime principles:

a. **Transparency:** Transparency requires defining clearly and narrowly the content that is blocked or prohibited; this informs content providers of what material is not permitted and helps citizens understand the values that filtering seeks to implement.

b. Inclusiveness: Inclusiveness requires a system/mechanism or a body responsible for the decision-making about filtering, that keep a check and balance of the appropriate material, that take the requests and feedback from the public and is eligible of taking necessary decision on

blocking/unblocking of the requested content, after analysis. That body is accountable to their decisions by the legislature.

c. Credibility: Credibility requires a system, which keeps track of the up gradation of the system with increasing requirements, periodic updating of filtering categories, implementation check at all the tiers and levels of filtering implementation (ISPs and landing stations etc).

3. Proposed Filtering configuration/ mechanism

a. It is proposed that, in order to meet International requirements up till 2012, the mass level filter solution having the monitoring capability of at least 40Gbps of traffic, on each interface of filter, be applied at the International gateways, i.e. following a centralized approach* for filtering . This configuration will let all users experience the same degree of filtering and is more feasible solution. The advantage of Centralized filtering approach is, high consistency which is hard to achieve in distributed configuration,

**Note: The comparison of centralized vs. Distributed and the adopted models of multiple countries is discussed in Annex below.*

b. The **technical capability** of the solution should be such that introduces minimum delays, may be around 32 micro seconds or less, support multiple languages and must filter through IP addresses, URLs, protocols, proxies and viruses.

c. The equipment at the International gateway should have a well **defined filtering database** with standard categories. The lists are customizable list and one can always add or remove the categories of choice.

There is an option of borrowing a Database from 3rd party. Few concerns in borrowing the 3rd party DB are,

a. Handsome annual fee of DB,
b. Complete reliance on the other country for national filtering process and
c. The threat of leakage of the national blocking policies and blocked/filtered content.

d. Database encryption is an essential feature of security of block list.

e. If distributed system is applied, then all the ISPs will have to be enforced to apply the filtering system and abide by the filtering Laws, and a strict supervision is required by the Government Body to maintain consistency of filtering.

1.5. Cost of solution, capacity building, socio-political implications and other ancillary aspect of proposed mechanism implementation.

1.5.1. Cost of solution for a Centralized configuration

In general, URL filtering solutions can work independently or can be integrated with other network components such as Caches, Packet Inspection nodes and security devices. And hence price/ cost of solution depend on architecture adopted.

For a traffic of 150 Gb/s capacity, with most of the above mentioned features, in a centralized configuration, with no additional components i.e. only the filter module, may cost around 5Million to 7Million dollars without redundancy.

1.5.2. Capacity building of Proposed System

1. **Hardware & software expansion:**
   i. In the phase-1, the hardware with almost 50% higher than the current international capacity may be deployed at the landing stations. It may be noted that, as long as the cache servers are not behind the filtering wall, the target of filtering cannot be achieved. Hence the filtering would be done such that both the landing station and the cache servers are filtered.
      i. In the second phase all the ISPs may be provided with the small scale (ISP level) filtering solution and made to follow the code of practice.

   ii. In the software up gradation, version up gradation should be automatically upgraded by the vendor as soon as the upgrade is available. Whereas the updating in the Dynamic category list will be periodic, in pace with the rapid changes in internet trends and traffic.

2. **Management**
   i. **High level management:** This group could either be a full fledge separate entity within GoP responsible for heading the entire web related decision making or it could be an inter-ministerial committee formed through participation of all stakeholders headed by someone directly reporting to the PM.
   ii. **Low Level Committees:** The low level committees may then be established again as separate entities as representatives of several stakeholder organization to look after the finer details specific to their expertise.
   iii. **Team:** It will be required to formulate a team of skilled persons, who would serve as internet watch dogs, manually check and scan the traffic, identify the undesired and evaluate any URL, requested or identified, for blocking/unblocking. This team will expectedly expand with the expansion of the web traffic

1.5.3. Socio-Political Implications & Ancillary Aspect of Proposed System

1. National filtering is seen as a technical "quick fix" to much of the broader social and cultural problems that arise from larger social and political issues.
2. Often observed in several states that implement filtering to target adult content has extended such a capability to block content for political reasons as well. Often, governments have extended filtering to silence criticism, control political uprising and indigenous state violence online.
3. If filtering is imposed through interpretation of vague laws and regulations, there is little transparency regarding the selection of sites to block or unblock, and the politically motivated can exploit such a situation.
4. Filtering technology cannot block all content that governments intend to block and it may lead to blocking of content that was never intended to be blocked. These false blockings and unblocking often have serious implications for both freedom of speech as well as the normal functioning of the Internet. However, this is sort of a fundamental flaw and unless the governments are not careful enough, it may lead to different circumvention methodologies.

2. Mechanism for sharing information / database of Internet Café in Pakistan:

2.1. Analyze international best practices to curb under-age/children exposure to pornographic content/ child abuse and terrorism through points of shared access like internet cafés

Countries in the world have regulated the cyber cafes to some extent and in some instances, there are quite strict regulations on the cyber cafes. The cyber cafe crimes specially for the children is a raising concern round the globe. Many countries have not touched this sensitive topic of cyber cafe regulation/control as yet. Few of the countries having defined rules to regulate cafes are discussed below.

1. Nepal:

During 2011, Nepal Telecommunications Authority (NTA) has instructed all cyber cafes through their Internet Service Providers (ISP) to keep detailed record of their customers, including name, permanent and temporary address of the customers, also verify the details by checking the government issued identity cards such as driving license, citizenship certificate or passport, before letting them use the internet. NTA has asked the ISPs to ensure such provision is implemented strictly by three months. CWIN (Child Workers in Nepal) takes initiative to start a project/campaign to address the issue of online child protection. (CWIN) is a non-Government organisation in Nepal for the rights of the child and child protection. It take initiatives of projects/campaigns to address the issue of online child protection.

2. Philippine:

An ordinance prescribing guidelines and regulations on the operation and services of internet Cafe and other similar establishments for the protection of children, and for other purposes is in effect, Which applies following on cyber cafes:-

1. Prohibition against installation of private cubicles or rooms
2. Posting of internet safety rules and cyber ethics principles in a visible place and in every open cubicle
3. Firewall and Content Control
    i. Internet cafés shall provide their own firewall software o control the type of content accessed through the internet
    ii. Install filtering software that inhibits access to pornographic websites
4. Internet user's logbook
    i. Maintain an internet user's logbook containing the name of the user, age, address, login and logout times, and signature.
    ii. All users shall be required to show a valid ID to validate this information

3. Hong Kong

There are certain specific conditions for the cyber cafes in Hong Kong. Like, Internet cafe Operator is required to give notice of its establishment to the relevant authority, Some specific conditions on the child protection, Maintain a log of users with valid photo-identity cards, Install filtering software so as to block sex and gambling websites. Install devices to screen violent, pornographic or gambling websites. Minors are not be allowed to use computers in cubicles or behind partitions, the screens should be visible to passers-by, Youth are not allowed to stay at internet cafes after 10pm without permission . Failure to comply with these conditions could result in suspension or termination of business.

4. UAE

1. Written approval from Ministry of Culture and Community Development to operate an internet cafe
2. Valid trade license from the Economic Department or the Municipality of the Emirate Passport copies of the owner and service agent
3. Copy of tenancy contract for the internet cafe
4. Copy of power of attorney (if applicable)
5. Letter from the owner of the business stating the identity and qualifications of the person managing the internet cafe

a. The internet content is filtered in UAE by a sophisticated filtering mechanism and all the cafes are registered with the authority and are bound to abide by the cyber laws.

2.2. Current record of number and location of Internet Cafés/multi-purpose community centres/ Tele-centres as well as occurrence of Cyber crimes / Terrorism activities originated from Cyber cafés

No such data is available for Pakistan.

2.3. Capacity building, socio-political and other ancillary aspect of proposed mechanism implementation.

2.3.1. Capacity building

This subject has already being discussed in detail in an earlier heading.

2.3.2. socio-political

In addition to what has already being discussed earlier, failure to regulate cyber cafes may have a far reaching impact on the socio-political screen of Pakistan. The negative impact would simply be considered to an order of magnitude higher than what otherwise be experienced in a residential and business environment. It is recommended that we follow an optimal approach comprising of all those elements contained in UAE, Hong Kong and Philippine, except that the privacy to the content of the user should be respected.

1. Recommendations

1.1. A Gigabyte capacity filtering solution may be implemented on the International Gateways. That is a centralized filtering configuration be implemented across country.

1.2. A clear document defining the objectionable and block able content may be provided by the concerned government body.

1.3. All the ISPs, cashes owners and blog owners (blogs hosted in Pakistan) to mandatorily implement secondary level filtering mechanism. And maintaining ID logs of their users.

1.4. System should be in place to clear all caches within Pakistan as and when required.

1.5. The bock List, generated by the special committee formed for the purpose, should be directly downloadable to all the filtering systems without any further human interference.

1.6. The system be able to revisit the blocked sites and update accordingly.

1.7. False blocking may be reviewed by a human rescores team, self scanning and also on the public user's

requests.

2. Reference

http://www.internet.gov.sa/learn-the-web/guides/content-filtering-in-saudi-arabia
http://www.isoc.org/inet97/proceedings/B1/B1_3.HTM
http://www.scribd.com/doc/51812915/ONI-WestCensoringEast
http://opennet.net/sites/opennet.net/files/ONI_Country_Study_Singapore.pdf
http://opennet.net/research/profiles/iran
http://cdn.gotoknow.org/assets/media/files/000/642/840/original_ChildProtectionSysteminICTofThailand.pptx?1289279870
http://www.worlddialogue.org/content.php?id=400
http://ojphi.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227

1. * ISPs: Most of the countries which impose regulations on ISPs have very few ISPs in their country.

Terms of Reference:

i. Mechanism for content filtering over internet in Pakistan:

   a. Analyze international best practices for blocking pornographic / anti state content over internet and role of ISPs/Operators worldwide;

   b. Analyze effectiveness of mass level technical filtering, its limitations and repercussions of censorship and propose mechanism in the light of the current capabilities;

   c. Cost of solution, capacity building, socio-political implications and other ancillary aspect of proposed mechanism implementation.

ii. Mechanism for sharing information / database of Internet Café in Pakistan:

   a. Analyze international best practices to curb under-age/children exposure to pornographic content/ child abuse and terrorism through points of shared access like internet cafés;

   b. Current record of number and location of Internet Cafés/multi-purpose community centers/Telecenters as well as occurrence of Cyber crimes / Terrorism activities originated from Cyber cafés;

   c. Capacity building, socio-political and other ancillary aspect of proposed mechanism implementation.

Countries Case Study

1.1. China

Great Firewall of China

China promoted the development of Internet infrastructure and services while strictly regulating flow of unwanted content.
China's Internet filtering system—known as "the Great Firewall of China" officially known as the Golden Shield Project —is probably the most sophisticated , domestically developed and extensive in the world, implemented on the international gateways and regulated at each stream down to each cyber café assuring filtering from head to toe. Its designing began in 1998 and became operational in November 2003.

a) There are more than sixty Internet regulations made by the Chinese government and censorship systems which are vigorously implemented by provincial branches of state-owned ISPs, business companies, and organizations.

b) This project costed $800 million and an updated version was built between 2006 and 2008.

c) Cybercafés are required to keep detail logs of customers' online activity on file for 60 days. If a user tries to access forbidden Web sites, a café must disconnect the user.

d) Cyber services cannot be used without an identification card, a copy of which is kept on record for at least 60 days. Children under 16 are not allowed in cybercafés.

e) Their Filtering system blocks URLs based on 13 categories.

1.1.1. Cyber Cafes and ISPs in China

In addition to the broad range of content filtered at the international gateways , domestic providers as to remain in regulatory compliance are required to install internal filtering mechanisms and devote staff resources to monitor content on their internet traffic/Web sites or otherwise face civil and criminal liability.

a) The size of the Internet Police is rumored at more than 50,000. Critical comments appearing on Internet forums, blogs, and major portals usually are erased within minutes.

b) China has cultivated a model that protects a broad filtering regime by strictly regulating its own content providers, allowing it to maintain more optimal levels of control over its expansive domestic content market.

1.1.2. Self Censorship in China

a) The Chinese government delegated the content monitoring role to Internet Service Providers (ISPs), search engines and even blog service providers and instant messaging software programs by requiring them to search and filter content.

b) ISPs are held legally responsible for any unwanted content that is able to be displayed through their service.

1.2. Saudi Arabia

- The internet filtering service started with the introduction of Internet in the Kingdom of Saudi

Arabia. The Council of Minister, *in March 1997,* assigned the provision of Internet services in the Kingdom to Internet Services Unit of a scientific organization ,*'King Abdulaziz City for Science and Technology*'. The responsibilities of the Internet Services Unit was to implement the required Internet content filtering for International Internet traffic along with other responsibilities, as all the internet traffics pass through the servers of the Internet Services Unit.

- **Committee for filtering Policies:** A Permanent Committee headed by a Ministry, including representatives from the concerned ministries and entities was formed to develop the filtering policies and to take the blocking/unblocking decisions.

- **Communications and Information Technology Commission (CITC)**

In the Y2004, the Internet filtering service was transferred to the Communications and Information Technology Commission (CITC) to develop measures and requirements, and provide the blocked sites daily database to data service providers, which in turn block the list through a filtering technical solutions, in accordance with CITC requirements and policies.

The filtering process is conducted through 2 lists:

a) Static List
b) Dynamic List

a) Static List, by International Company:

CITC has contracted with an International Company specialized in sites classification, to provide the commercial list, which is implemented at international traffic Gateway to block undesired content. The includes more than 90 different classifications/categories. The list is updated by the company on regular basis. In addition there is a continuous communication between CITC and the company to avoid any error in rating classification.

b) Dynamic List, Public requested sites

The local list is prepared by CITC through the addition of sites that are recommended by public users, after reviewing and ensuring, that such sites contains illegal material. The URLs added to local list rated sites can be classified according to the content as following:

a. Pornographic sites, which represent 92.80% of the local list.
b. Sites that could not be filtered at 1.2.a nor part of 1.2.b.a, represents 4.43% of the local list.
c. Other sites (such as: gambling, drugs, magic...) which represents 2.77% of the local list.

Requests are received from public users through the blocking/unblocking special forms. A ticket is opened for each request. URLs will be added only after being reviewed by CITC. The sites that fall under the CITC responsibilities are added directly to local list, all other requests are submitted to the committee for study and decision. This list is updated after intervals , based on the content filtering policy.

1.2.1. Data Service Providers/ISPs in Saudi Arab

The Local Lists containing the blocked sites database are forwarded periodically to data service providers, which in turn initiate blocking.

1.3. Singapore

Singapore has applied state filters to Internet content, to promote social values and maintain national unity, with the goal of denying access to objectionable material, especially pornography and content encouraging ethnic or religious strife. The Media Development Authority (MDA) claims to block the unethical content. In addition, the MDA encourages, and each of Singapore's three primary Internet Service Providers offers, optional, filtered Internet access services that block additional sites for a minimal monthly fee. A survey

during the Y 2006 by OpenNet Initiative (ONI), found extremely minimal filtering of Internet content in Singapore. The limited blocking focuses on a few pornographic URLs and one site each in the categories of illegal drugs and fanatical religion. Similar content is readily available at other sites on the Internet that are not blocked in Singapore. Thus, Singapore's Internet content regulation depends primarily on access controls (such as requiring political sites to register for a license) and legal pressures (such as defamation lawsuits and the threat of imprisonment) to prevent people from posting objectionable content rather than technological methods to block it. Compared to other countries that implement mandatory filtering regimes, Singapore's technical filtering system is one of the most limited.

The mainstream media is filtered by state filter, while alternative media such as independent Web sites and blogs are regulated through "light touch" regulatory framework having a class license scheme that requires:-

a) All ISPs and ICPs (Internet commerce providers) determined to be political parties or persons "engaged in the propagation, promotion or discussion of political or religious issues relating to Singapore to register with the Media Development Authority.

    a. Thus, individuals, groups, and other organizations engaged solely in the discussion of these issues online must register for a license.

b) However, the class license scheme has been rarely enforced, achieving greater efficacy in cultivating what its critics call a "culture of silence" through self-censorship.

In April 2007, the Singaporean government created an advisory council to study and make recommendations on its regulatory regime for "interactive digital media."The Advisory Council on the Impact of New Media (AIMS) report, issued on December 8, 2008, praised the longstanding "light touch" approach to regulation of new media, while proposing some incremental changes. For example, AIMS recommended that the registration requirement for political parties be eliminated, but also argued that the Class License Scheme be preserved.

1.4. Iran

Islamic Republic of Iran now employs domestically produced technology for identifying and blocking objectionable Web sites, reducing its reliance on Western filtering technologies. Some within Iran were concerned that Western software might include a 'backdoor' that would give outsiders access to key infrastructure.
Speech in the Iran is heavily regulated. speech restrictions extend over a broad range of topics, including religion, immorality, social harmony and politics. Speech regulation in Iran is rooted in its constitution, which declares that "the media should be used as a forum for healthy encounter of different ideas, but they must strictly refrain from diffusion and propagation of destructive and anti-Islamic practices."

The implementation of the filtering decisions is charged to a filtering division within the Information Technology Company of Iran (ITC), an agency under MICT.22 Another agency, the Communication Infrastructure Company, has been given the task of unifying filtering across Iran.

Filtering is implemented by routing all public Internet traffic through proxy servers. This allows the employment of filtering software to target specific Web pages as well as the blocking of keywords. The blocking of Web sites is carried out in a transparent manner.

Applying strict principles to the Internet, with 20 million people on the Internet, currently the second highest percentage of its population online in the Middle East, after Israel, has proven to be difficult. A number of government regulatory initiatives have been launched over the past decade to assert control over online communications.

1.4.1. ISPs & Data Service Providers in Iran

    a. Every ISP must be approved by both the Telecommunication Company of Iran (TCI) and the Ministry of Culture and Islamic Guidance, and must implement content-control

software for websites and e-mail.

b. ISPs face heavy penalties if they do not comply with the government filter lists. At least twelve ISPs have been shut down for failing to install adequate filters.

1.5. India

Authorities are implementing stricter surveillance and monitoring controls over Internet activities. Tata Communications, formerly known as Videsh Sanchar Nigam, announced in 2007 the launch of Tata Indicom's Web Protect, which in collaboration with Netsweeper "enables users to block access to specific websites, chat rooms or any other unwanted content."

To enforce mandatory censorship. The other Indian telecom provider, BSNL (Bharat Sanchar Nigam Ltd.), uses the Filter as the interceptor, with all the network traffic going through the filter.

The Government of India is cracking down on illegal content on web sites. BSNL, India's largest telco has implemented technology to meet Federal content regulations.

1.6. Syria:

In Syria, ISPs such as Inet, Teranet, and Zad have used Squid as aproxy tool to block access to objectionable websites that included oppositional Web content. Squid is a free software package released under the GNU General Public License that was funded by the National Science Foundation.

It is a caching proxy that is built to reduce bandwidth and improve response times by caching and reusing frequently-requested Web pages, however, ISPs in Syria have repurposed it for Internet censorship.

1.7. Australia

Internet censorship laws were passed by the Federal Commonwealth Parliament in 1999 and commenced operation on 1 January 2000. The Broadcasting Services Act was amended to give the television regulator, the Australian Broadcasting Authority ("ABA"), the power to order Australian ISPs to remove content hosted on their networks, including Usenet messages. It also provides the power to the ABA to order Australian ISPs to take-down images and text from websites and newsgroup servers on threat of fines of up to AUD$27,500 per day.

Annex C

Proposed Capabilities of Mass Level Technical Filter:

In general, URL filtering solutions can work independently or can be integrated with other network components such as Caches, Deep Packet Inspection nodes and security devices.

Deployment of URL filters can either be centralized or distributed depending on the service provider. ISP's are best suited for a distributed deployment. On the other hand, Internet gateway providers (aggregates of Internet traffic) are best suited for a centralized deployment.

Following are few of the proposed technical capabilities for a mass level filtering solution.

	Characteristics	The solution should support :-	Comments
1.	Filtering/ Blocking	URL Filtering and Blocking	From domain level to sub folder and file levels
2.		IP Address/Range Blocking	Can block a single IP address or a Range of IP address
3.		Protocol based blocking like FTP, Telnet, SMTP etc.	
4.		Block Proxy Access of Blocked website	
5.		Composite Blocking like FTP Service on a particular IP	
6.		Virus attacks	handle DDOS attacks and also scan for viruses.
7.			
8.	System	Stand Alone HW	That can be integrated into any Ethernet/IP network
9.		DPI Performance (if Yes, what level)	
10.		Network Configuration (Inline/out)	Should be in line with the data path in order to monitor on a fly
11.		Operates on OSI layer	
12.		Scalable capacity	Should be saleable to address filtering requirements up to three years at least.
13.		Cashing coupled with Filtering	For enhancing filtering performance
14.		Ability to intercept the flow in both directions (in-bound or out-bound traffic)	Should have ability to filter in both directions.
15.		Programmable	Rapidly programmable to support new protocols and applications
16.			

17.			
18.			
19.	Speed & Delays	Overall introduced Latency (sec) (max)	32 micro sec per request
20.		Total number of URLs inspected at a time Or Max. Concurrent Unidirectional filtering Capacity	100,000 filter requests per second
21.		Supported languages	should support multiple languages to capture URL in any language
22.	Database	Uses external Database(IWF etc)	Must support IWF or any other equivalent 3rd party URL DB
23.		Master Database Update Time	
24.		Master Database Geo location.	Better have Locally installed & maintained database?
25.		No. of Inbuilt categories	
26.		Proprietary DB	Should allow Proprietary DB definition or integration
27.		Filter DB Flexibility	DB be Locally Modified to meet customer needs
28.	Filter BD Categories	No. of Categories in Local Database	
29.		Allowed no. of Category definitions by solution holder	
30.		No of filtering categories defined in Master DB	
31.		Filter DB Flexibility	should be flexible to add/ remove filters or categories
32.	Back-end Control	who all have View Access to blacklist URL database	Only the solution holder should have the access to view its block categories. The indigenous solution is this aspect is suggestible. Otherwise the vendor should not have access to view the categories defined by customer. This is in National interest.
33.	Support	Support Office In/Outside Pk	Support office should be in Pakistan or wither wise in some nearby countries. Better if local support is available
34.			
35.	Commercial	O&M	The system should have 5 year O&M contract or MoU.
36.	Security	DB Access	No one can view or access the customer defines categories

37.		Agency Clearance	Must be agency cleared
38.	Filter BD Categories	No. of Categories in Local Database	
39.	Added On Features		
40.	System	Hardware fast-path	separate hardware path for delay-sensitive traffic, ensuring very low latency (~10micS)
41.	DB	Updating Database	Updating this URL DB done through CLI commands
42.	DB	DB encryption/ security	Blacklist database protected with AES encryption key
43.			

Centralized Deployment

Centralized filtering regime at Gateway require all Internet traffic to pass through the same filters. This results in a consistent view of the International Internet content for users within the country; all users experience the same degree of filtering. This configuration is best suited for Internet Gateway providers since they aggregate ISP Internet traffic with International uplink providers.

1. Distributed Deployment:

When filtering is delegated to the ISP level, and hence decentralized, there may be significant differences among ISPs regarding the filtering techniques used and the content that is filtered. This configuration is best suited for ISPs with distributed exchange offices (Points of Presence) that have varying customer populations.

Feature	Centralized Model	Distributed Model
Consistency	Easy to achieve	Requires authorities to play their role
Investment	High	Distributed / comparatively low
Filtering Solution	Very high processing & throughput	Low processing & throughput
Quality Management	Very high capacity requirement for good Quality requirement	Delegated to ISP level. Strict supervision required.
Dependency	Single vendor, Indigenous solution can provide resolution	Multi vendor . Indigenous solution shall provide resolution.
Point of failure	Single	Distributed
Filtering of Local Content	Not possible	Possible

3. PTCL feedback on Cyber Cafe

3.1. The general response of the industry (ISP/ BSP only) on a consultation on Soft Touch Cyber Café Regulations.

3.1.1. Registration Of Cyber Cafés with Regulator or ISPs?

They must be registered and regulated by Govt Authorities / PTA, as ISPs do not have the resources to police them for this.

3.1.2. Mandatory agreement between ISP and Cyber Café

Only commercial and SLAs agreements between Cyber Cafés and ISPs. The Regulator should enforce Policy to be followed by both ends.

3.1.3. Type of the records cafe owner should keep, and for how long?

User Activity records may be kept by Café for min 3 Months. ISPs should not be included in record keeping.

3.1.4. Run under ethical n constitutional obligations.

Strict Regulatory Policy be enforced to check unethical use of cafés.