Part VII: Content monitoring: The debate continues

Internet makes it possible for communities to interact and share knowledge, information, voice and visual content freely, leading to creative social re-organisation. Internet is thus as much a social phenomenon as it is technological. With the evolution of the Internet in its new phase, commonly called Web 2.0, cyber communities and social access to Internet has been enhanced. According to Diplo Foundation, in its primer on Internet Governance, talks about this content and related issues, as the most controversial in the field of Internet Governance[3]. Content policy, spam and filtering, public goods perspectives, etc., are being taken up in various debates across the world.

In this issue, we try to understand the nuances of the various aspects of content monitoring. The content policy has to be seen both from the point of view of human rights (freedom of expression and the right to communicate), government (content control) and technology (tools for content control).

International issues where there are major agreements

Issues like child pornography, genocide, incitement or terrorism related content, as prohibited by international law are not so contentious. There is wide ranging agreement that such contents should be removed from the Net, but there is not a consensus on how to interpret these. Another group of issues centres on content that is sensitive to different countries, ethnic minorities, or regions, due to their specific cultural contexts or values. There is a third group of issues revolving around political and ideologically sensitive content. This, in common parlance is referred to as Internet Censorship. Transparency International[8], headquartered in Berlin, has reported a number of such practices in China, Myanmar, Saudi Arabia, etc.

Content Control vs Freedom debate

Many organisations that want to share information only among peers or are worried about the safety and security of the data/content would like to explore issues relating to information security. Information security is a domain that worries not only technology providers but also businesses and governments in various countries.

The content policy in the Internet Governance domain relates not only to public (governmental) filtering of content, private rating and filtering systems, controls through search engines and geo-location software, but also through international legal framework developed by different regions, like the European Union.

The issues are raised by Human Rights organisations include the issues of privacy, freedom of expression, the right to receive information, various rights protecting the cultural, linguistic and minority diversity, and the right to education.

The Intellectual Property Rights (IPR) allows anyone to enjoy protection of the moral and material interests from scientific, literary or artistic production. The World Intellectual Property Organisation (WIPO)[2] is the global body empowered to set the norms for IPR issues. This has, in the recent years, responded to a number of civil society and advocacy groups' call for a developmental perspective to be built, keeping in mind the rights guaranteed by the Article 19 of the UN Human Rights Declaration. A point to note is the counter-balance in the Article 29 which gives the right of the state to limit freedom of expression for the sake of morality, public order, and general welfare.

The main challenge is to establish a balance between these two schools of debate on the content policy with respect to Internet Governance.

How do governments filter content on the Internet?

Governments often engage in creating an Internet Index of websites blocked for access by citizens. If a website is in this index, it will not be accessible to its citizens. Technically, the filtering typically uses router based IP blocking, proxy servers, and DNS redirection. Many countries track and monitor websites frequently. Some countries known to practice this extensively include China, Saudi Arabia, Myanmar, Singapore, but also other countries like Australia, Germany, France, USA, UK, etc [1]. Such national filtering systems pose the risk of disintegration of the Internet in its spirit of free flow of information. W3C had suggested that rather than using the national filtering process, the end users should be encouraged to implement a rating and filtering system. Such browser level filtering is very useful to make end-user computers, child friendly, for example.

Some search engine companies like Google impose self-censorship. For example, in their German and

i4d
Information for development
In Collaboration with:
nixi
National Internet eXchange of India
www.nixi.in

French versions of Google, it is not possible to search for and find websites with Nazi materials. This is usually done to avoid possible court cases.

Even in India, recently, sites like Orkut and YahooGroups have faced temporary shutdowns due to controversial content. The Indian government has stepped in after public outcry and not suo moto.

According to Naresh Ajwani, Secretary, Internet Service Providers Association of India (ISPAI), "ISPs are not Police but the facilitators of content flow on the Internet. It's like saying that the TV manufacturers like LG/Samsung shall be responsible for channels' content...Having said that ISPs must act over any advised information from the law enforcement agencies to check on any content provider"

Normal websites, or static websites are often moderated and managed by organisations. Whereas, personal blogs which use web 2.0 technologies, and other user related contents are often un-restricted information floating in the Internet space. The community and social networking sites offer space for content creation, and define the general norms for the type of content that can be placed.

Other sites use a polling tool to report or flag unsuitable content. These sites may remove messages that have been flagged by other members are insensitive or objectionable content. This is a type of moderation that allows peer ranking of content. Other sites like eBay deletes references to 'soul' for sale or other similar irrelevant content posted by its members.

Whether it is self-monitoring, or peer-review or regulation by government, the issue of content monitoring has both technological and legal perspectievs.

The technology perspective

Gartner released its "Magic Quadrant for Content Monitoring and Filtering and Data Loss Prevention, 2008"[5] a report by Gartner analysts Eric Ouellet and Paul E. Proctor. The rep ort states, "We have long believed that integrated network, endpoint and discovery capabilities - with a centralized management console capable of distributing a consistent set of policies, and providing usable event analysis and workflow for alerting on and remediating violations - was the ultimate goal and destination of this market."

Gartner, Inc.'s Magic Quadrant positions vendors in a particular market segment based on their ability to execute and completeness of vision. The report explains that "leaders have demonstrated a good understanding of client needs and offer comprehensive capabilities in all three functional areas, including network, discovery and endpoint directly or through well-established partnerships and tight integration. They offer aggressive road maps, but they will need to execute on those road maps, fully incorporate enhanced features being developed and address evolving market needs to remain in the Leaders Quadrant."

Though this is a research tool, and not an endorsement, it is one of the most respected analysis for assessing the security tools and technologies for organizations looking for solutions to secure their data and content.

Global legal initiatives

There is a legal vacuum in the field of content monitoring and policies around it. While governments use high levels of discretion in content control, it is important to recognize the need for global discussions and consensus building on this issue. Some of the initiatives towards this are discussed below:

The Council of Europe Additional Protocol on the Cybercrime Convention specifies various types of hate speech, including racist and xenophobic materials, justification of genocide and crimes against humanity that should be prohibited on the Internet. The Organisation of Security and Cooperation in Europe (OSCE) is particularly active in this field. It aims to reduce censorship and promote freedom of expression on the Internet. Practically, the EU has introduced the EU Safer Internet Action Plan[6] which includes:

- setting up of a European network of hotlines for reporting of illegal content,
- encouraging self-regulation,
- developing content rating, filtering, and benchmark filtering,
- developing software and services, and
- raising awareness of safer use of Internet.

It also encourages the concept of what is illegal offline, is illegal online, though enforcement is more difficult of material posted on, and shared through the Internet.

The Internet Watch Foundation[7] in UK aims at combating child abuse on the Internet, and works with several stakeholders to promote its cause. Though the main players will continue to be governments, the role of communities, parents, schools etc. are also important when it comes to child safe content.

Internet should also be protected as a global public good, with two key properties, viz., non-rivalrous consumption and non-excludability. At the legal level, the concept of res communis omnim (space as a common heritage of humankind to be regulated and garnered by all nations), is being promoted to further the concept of Global Public Good. The concept of the "commons" is another term which is used to define Internet Content.

It is important to note that the debate is ongoing and will continue to be discussed at the upcoming Third Internet Governance Forum to be held in Hyderabad from December 3-6, 2008. For further details, please log on to *www.intgovforum.org*

References:

1. *http://www.efa.org.au/Issues/Censor/cens3.html*
2. *www.wipo.int*
3. Internet Governance: Issues, Actors and Divides (2005), edited by Eduardo Gelbstein and Jovan Kurbalija, DiploFoundation, Malta *http://www.diplomacy.edu/ISL/IG/default.htm*
4. *www.intgovforum.org*
5. Gartner Magic Quadrant: *www.gartner.com/it/products/mq/mq_ms.jsp*
6. *www.osce.org*
7. Internet Watch Foundation: *www.iwf.org.uk*
8. Transparency International: *www.transparency.org*