Internet Governance and Censorship

Osbaldo Fuentes
Maryjane Wren

First Edition, 2012

ISBN 978-81-323-1283-3

Published by:
College Publishing House
4735/22 Prakashdeep Bldg,
Ansari Road, Darya Ganj,
Delhi - 110002
Email: info@wtbooks.com

Table of Contents

Chapter 1

Introduction to Internet Governance

Policies and mechanisms for **Internet governance** have been topics of debate between many different Internet stakeholders, some of whom have very different opinions for how and indeed whether the Internet should facilitate free communication of ideas and information.

Definition

The definition of Internet governance has been contested by differing groups across political and ideological lines. One of the main debates concerns the authority and participation of certain actors, such as national governments, corporate entities and civil society, to play a role in the Internet's governance.

A Working group established after a United Nations-initiated World Summit on the Information Society (WSIS) proposed the following definition of Internet governance as part of its June 2005 report:

Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

Law professor Yochai Benkler developed a conceptualization of Internet governance by the idea of three "layers" of governance: the "physical infrastructure" layer through which information travels; the "code" or "logical" layer that controls the infrastructure; and the "content" layer, which contains the information that signals through the network.

History

To understand how the Internet is managed today, it is necessary to know some of the main events of Internet governance.

The original ARPANET, one of the components which evolved eventually into the Internet, connected four Universities: University of California Los Angeles, University of California Santa Barbara, Stanford Research Institute and Utah University. The IMPs,

interface minicomputers, were built during 1969 by Bolt, Beranek and Newman in accord with a proposal by the US Department of Defense Advanced Research Projects Agency, which funded the system as an experiment. By 1973 it connected many more systems and included satellite links to Hawaii and Scandinavia, and a further link from Norway to London. ARPANET continued to grow in size, becoming more a utility than a research project. For this reason during 1975 it was transferred to the US Defense Communications Agency.

During the development of ARPANET, a numbered series of Request for Comments (RFCs) memos documented technical decisions and methods of working as they evolved. The standards of today's Internet are still documented by RFCs, produced through the very process which evolved on ARPANET.

Outside of the USA the dominant technology was X.25. The International Packet Switched Service, created during 1978, used X.25 and extended to Europe, Australia, Hong Kong, Canada, and the USA. It allowed individual users and companies to connect to a variety of mainframe systems, including Compuserve. Between 1979 and 1984, a system known as Unix to Unix Copy Program grew to connect 940 hosts, using methods like X.25 links, ARPANET connections, and leased lines. Usenet News, a distributed discussion system, was a major use of UUCP.

The Internet protocol suite, developed between 1973 and 1977 with funding from ARPA, was intended to hide the differences between different underlying networks and allow many different applications to be used over the same network.

RFC 801 describes how the US Department of Defense organized the replacement of ARPANET's Network Control Program by the new Internet Protocol during January 1983. During the same year, the military systems were removed to a distinct MILNET, and the Domain Name System was invented to manage the names and addresses of computers on the "ARPA Internet". The familiar top-level domains .gov, .mil, .edu, .org, .net, .com, and .int, and the two-letter country code top-level domains were deployed during 1984.

Between 1984 and 1986 the US National Science Foundation created the NSFNET backbone, using TCP/IP, to connect their supercomputing facilities. The combined network became generally known as the Internet.

By the end of 1989 Australia, Germany, Israel, Italy, Japan, Mexico, the Netherlands, New Zealand, and the United Kingdom had connected to the Internet, which now contained over 160,000 hosts.

During 1990, ARPANET formally terminated, and during 1991 the NSF ended its restrictions on commercial use of its part of the Internet. Commercial network providers began to interconnect, extending the Internet.

Today almost all Internet infrastructure is provided and owned by the private sector. Traffic is exchanged between these networks, at major interconnect points, in accordance with established Internet standards and commercial agreements.

Actors

During 1979 the Internet Configuration Control Board was founded by DARPA to oversee the network's development. During 1984 it was renamed the Internet Advisory Board (IAB), and during 1986 it became the Internet Activities Board.

The Internet Engineering Task Force (IETF) was formed during 1986 by the US Government to develop and promote Internet standards. It consisted initially of researchers, but by the end of the year participation was available to anyone, and its business was performed largely by email.

From the early days of the network until his death during 1998, Jon Postel oversaw address allocation and other Internet protocol numbering and assignments in his capacity as Director of the Computer Networks Division at the Information Sciences Institute of the University of Southern California, under a contract from the Dept. of Defense. This function eventually became known as the Internet Assigned Numbers Authority (IANA), and as it expanded to include management of the global Domain Name System (DNS) root servers, a small organization grew. Postel also served as RFC Editor.

Allocation of IP addresses was delegated to four Regional Internet Registries (RIRs):

- American Registry for Internet Numbers (ARIN) for North America
- Réseaux IP Européens - Network Coordination Centre (RIPE NCC) for Europe, the Middle East, and Central Asia
- Asia-Pacific Network Information Centre (APNIC) for Asia and the Pacific region
- Latin American and Caribbean Internet Addresses Registry (LACNIC) for Latin America and the Caribbean region

In 2004 a new RIR, AfriNIC, was created to manage allocations for Africa.

After Jon Postel's death during 1998, the IANA became part of the Internet Corporation for Assigned Names and Numbers (ICANN), a newly created Californian non-profit corporation, initiated during September 1998 by the US Government and awarded a contract by the US Department of Commerce. Initially two board members were elected by the Internet community at large, though this was changed by the rest of the board during 2002 in a little- attended public meeting in Accra, in Ghana.

During 1992 the Internet Society (ISOC) was founded, with a mission to *"assure the open development, evolution and use of the Internet for the benefit of all people throughout the world"*. Its members include individuals (anyone may join) as well as corporations, organizations, governments, and universities. The IAB was renamed the Internet

Architecture Board, and became part of ISOC. The Internet Engineering Task Force also became part of the ISOC. The IETF is overseen currently by the Internet Engineering Steering Group (IESG), and longer term research is carried on by the Internet Research Task Force and overseen by the Internet Research Steering Group.

During 2002, a restructuring of the Internet Society gave more control to its corporate members.

At the first World Summit on the Information Society (WSIS) in Geneva 2003 the topic of Internet governance was discussed. ICANN's status as a private corporation under contract to the U.S. government created controversy among other governments, especially Brazil, China, South Africa and some Arab states. Since no general agreement existed even on the definition of what comprised Internet governance, United Nations Secretary General Kofi Annan initiated a Working Group on Internet Governance (WGIG) to clarify the issues and report before the second part of the World Summit on the Information Society in Tunis 2005. After much controversial debate, during which the US delegation refused to consider surrendering the US control of the Root Zone file, participants agreed on a compromise to allow for wider international debate on the policy principles. They agreed to establish an Internet Governance Forum, to be convened by United Nations Secretary General before the end of the second quarter of the year 2006. The Greek government volunteered to host the first such meeting.

Controversy

The position of the US Department of Commerce as the controller of the Internet gradually attracted criticism from those who felt that control should be more international. A hands-off philosophy by the US Dept. of Commerce helped limit this criticism, but this was undermined in 2005 when the Bush administration intervened to help kill the .xxx top level domain proposal.

When the IANA functions were given to a new US non-profit Corporation called ICANN, controversy increased. ICANN's decision-making process was criticised by some observers as being secretive and unaccountable. When the directors' posts which had previously been elected by the "at-large" community of Internet users were abolished, some feared the worst. ICANN stated that they were merely streamlining decision-making processes, and developing a structure suitable for the modern Internet.

Other topics of controversy included the creation and control of generic top-level domains (.com, .org, and possible new ones, such as .biz or .xxx), the control of country-code domains, recent proposals for a large increase in ICANN's budget and responsibilities, and a proposed "domain tax" to pay for the increase.

There were also suggestions that individual governments should have more control, or that the International Telecommunication Union or the United Nations should have a function in Internet governance.

Chapter 2

Alternative DNS Root and Domain Name Registry

Alternative DNS root

The Internet uses the Domain Name System (DNS) to associate the names of computers with their numeric IP addresses and with other information. The top level of the domain name hierarchy, the DNS root, contains the top-level domains that appear as the suffixes of all Internet domain names. The official DNS root is administered by the Internet Corporation for Assigned Names and Numbers (ICANN). In addition, several organizations operate **alternative DNS roots** (often referred to as **alt roots**). These alternative domain name systems operate their own root nameservers and administer their own specific name spaces consisting of custom top-level domains.

The Internet Architecture Board has spoken out strongly against alternate roots in RFC 2826.

Description

The DNS root zone consists of pointers to the authoritative domain name servers for all TLDs (top-level domains). The root zone is hosted on a collection of root servers operated by several organizations around the world that all use a specific, approved list of domains that is managed by ICANN.

Alternative roots typically include pointers to all of the TLD servers for domains delegated by ICANN, as well as name servers for other, custom top-level domains that are not sanctioned by ICANN. Some alternate roots are operated by the organizations that manage these alternative TLDs.

Alternative DNS roots may be characterized as three groups: those run for idealistic or ideological reasons, those run as profit-making enterprises, and those run internally by an organization for its own use.

While technically trivial to set up, the maintenance of a reliable root server network is a serious undertaking. In order for the system to be effective, multiple servers must be run continuously without interruption in geographically diverse locations.

During the dot-com boom, some alternate root providers believed that there were substantial profits to be made from providing alternative top-level domains.

Only a small portion of Internet service providers actually use any of the domains served by alternate root operators, generally supporting only ICANN-sanctioned root servers. This has led to the commercial failure of several alternative DNS root providers.

A `BIZ` TLD created by Pacific Root was in operation before ICANN approved the official `BIZ` domain, operated by Neulevel. For some time after the creation of the official domain, several alternate roots continued to resolve `BIZ` domains to Pacific Root's servers rather than Neulevel's. Therefore, some domain names existed in different roots and pointed to different IP addresses. The possibility of such conflicts, and their potential for destabilizing the Internet, is the main source of controversy surrounding alternate roots. Many of the alternate roots try to coordinate with each other, but many do not, and no conflict resolution processes exist between them.

List of alternative roots and their domains

This section lists the known alternate DNS roots, and for each root, lists the TLDs carried in addition to the ICANN-sanctioned gTLDs and ccTLDs.

Active public root zones

Public-Root

- Public-Root resolves multiple kinds of TLDs globally. It is created to offer an alternative, open DNS infrastructure with its own 13 root servers around the world.
- Administrated by INAIC
- Open for registration of new TLDs through an approved registrar, such as GQNET

OpenNIC

Public Access Website:

- `bbs` — aimed toward (Telnet style) bulletin board system servers, and affiliated/related/owned Websites.
- `dyn` — Approved by the OpenNIC Community, and will be introduced in mid-2008. Used to resolve dynamic DNS.
- `free` — non-commercial use of the Internet
- `fur` — Furry and Furry Fandom related sites

- `geek` — anything geeky
- `glue` — Sites related to infrastructure
- `indy` — Independent news and media
- `ing` — fun TLD. Further details to be confirmed
- `null` — miscellaneous non-commercial individual sites
- `oss` — Open source software
- `parody` — Parodies
- `eco` — Intended for the use in socially responsible investing (SRI) and ecological cooperatives, wholly owned subsidiaries, and other organisations that exist to promote or support the said co-operative.

New.net

Website:

- `agent`
- `art`
- `auction`
- `chat`
- `shop`
- `free`
- `golf`
- `llc`
- `llp`
- `love`
- `ltd`
- `school`
- `scifi`
- `soc`
- `video`
- `travel` — conflicts with ICANN-sanctioned TLD `travel`
- `tech`
- `kids`
- `church`
- `game`
- `mp3`
- `med`
- `mail`
- `xxx` — conflicts with TLD `xxx` which is in review by ICANN as of 2010
- `club`
- `inc`
- `law`
- `family`
- `sport`

UnifiedRoot

Website:

- UnifiedRoot enables all existing TLDs and allows new TLDs to be registered at a cost of €50,000 each (plus annual maintenance fees of €12,500).

UnifiedRoot offers a downloadable tool to modify the name server configuration on Windows. UnifiedRoot have also made agreements with ISPs and telcos to enable access to the provided TLDs. UnifiedRoot supports internationalized domain names (IDN) for top level domains (TLDs).

MobileTLD

Website:

- MobileTLD claims to resolve domains for mobile devices.

Open RSC

One of the notable challengers to ICANN's control of the DNS namespace was *Open RSC*, a group which grew out of private discussions and morphed into a public mailing list which grew large enough the group decided to submit an application to the US government to run the DNS.

Bylaws and articles of incorporation were posted outlining ORSC's position following extensive public discussion regarding the manner in which DNS was being run.

ICANN chairwoman Esther Dyson acknowledged adopting features such as membership from ORSC in her response to the US Department of Commerce.

ORSC publishes a root zone containing additional top level domains not found in the official root zone.

Website:

- `per` — personal pages
- `etc` — anything
- `web` — for the web
- `shop` — online shops
- `pickle` — just a general funny name
- `sco` — for Scottish culture
- `mail` - a tld for email - to reduce spam and clearly identify email servers.

Inactive public root zones

AlterNIC

AlterNIC ceased operation in 1997.

- `exp` —
- `llc` —
- `lnx` —
- `ltd` —
- `med` —
- `nic` —
- `noc` —
- `porn` —
- `xxx` —

eDNS

eDNS stopped in 1998.

- `biz` — General business use
- `corp` — For use by corporations
- `fam` — For and about Family
- `k12` — For and about Kids
- `npo` — Non-profit organizations
- `per` — Personal Domain Name services
- `web` — Web-based sites (ie: web pages)

Iperdome

Iperdome stopped in 1999.

- `per` — Personal Domain Name services
- later the TLDs changed to:
  - `biz` — General business use
  - `corp` — For use by corporations
  - `gay` — For and about the Gay Community
  - `k12` — For and about Kids
  - `npo` — Non-profit organizations
  - `pol` — Related to Poland and Polish organizations
  - `web` — Web-based sites (ie: web pages)

Open Root Server Network (ORSN)

(Shutdown 31.12.2008 00:00 UTC) Website:

- Used to be a mirror of the ICANN root.

Active private root zones

A number of organizations have alternative top-level domains configured on their internal DNS infrastructures, accessible only from within the enterprise. For instance, the National Security Agency operates the `nsa` domain; many NSA internal email addresses are of the form `username@r21.r.nsa`, mirroring the NSA organizational group structure.

Domain name registry

A **domain name registry** is a database of all domain names registered in a top-level domain. A registry operator, also called a **network information center** (NIC), is the part of the Domain Name System (DNS) of the Internet that keeps the database of domain names, and generates the zone files which convert domain names to IP addresses. Each NIC is an organisation that manages the registration of Domain names within the top-level domains for which it is responsible, controls the policies of domain name allocation, and technically operates its top-level domain. It is potentially distinct from a domain name registrar.

Domain names are managed under a hierarchy headed by the Internet Assigned Numbers Authority (IANA), which manages the top of the DNS tree by administrating the data in the root nameservers.

IANA also operates the .int registry for intergovernmental organisations, the .arpa zone for protocol administration purposes, and other critical zones such as root-servers.net.

IANA delegates all other domain name authority to other domain name registries such as VeriSign.

Country code top-level domains (ccTLD) are delegated by IANA to national registries such as DENIC in Germany and Nominet in the United Kingdom.

Operation

Some name registries are government departments (e.g., the registry for Sri Lanka *nic.lk*). Some are co-operatives of Internet service providers (such as DENIC) or not-for profit

companies (such as Nominet UK). Others operate as commercial organizations, such as the US registry (*nic.us*).

The allocated and assigned domain names are made available by registries by use of the WHOIS system and via their Domain name servers.

Some registries sell the names directly (like SWITCH in Switzerland) and others rely on separate entities to sell them. For example, names in the .com TLD are in some sense sold "wholesale" at a regulated price by VeriSign, and individual domain name registrar sell names "retail" to businesses and consumers.

Policies

Allocation policies

Generally, domain name registries operate a first-come-first-served system of allocation but may reject the allocation of specific domains on the basis of political, religious, historical, legal or cultural reasons.

For example, in the United States, between 1996 and 1998, InterNIC automatically rejected domain name applications based on a list of perceived obscenities.

Registries may also control matters of interest to their local communities: for example, the German, Japanese and Polish registries have introduced internationalized domain names to allow use of local non-ASCII characters.

Dispute policies

Domains which are registered with ICANN registrars, generally have to use the Uniform Domain-Name Dispute-Resolution Policy (UDRP), however, Germany's DENIC requires people to use the German civil courts, and Nominet UK deals with Intellectual Property and other disputes through its own dispute resolution service.

Prices of registration

Prices of domain registrations are set by each registry.

Third-level domains

Domain name registries may also impose a system of third-level domains on users. DENIC, the registry for Germany (.de), does not impose third level domains. AFNIC, the registry for France (.fr), has some third level domains, but not all registrants have to use them, and Nominet UK, the registry for the United Kingdom (.uk), requires all names to have a third level domain (e.g. `.co.uk or .org.uk`).

Many ccTLDs have moved from compulsory third or fourth-level domain to the availability of registrations of second level domains. Among them are .us (April 2002), .mx (May 2009), and .co (March 2010).

Domain Sub-Registration

Registrants of second-level domains sometimes act as a registry by offering sub-registrations to their registration. For example, registrations to `.fami.ly` are offered by the registrant of `fami.ly` and not by GPTC, the registry for Libya (.ly).

Chapter 3

Internet Governance Forum

Internet Governance Forum, Rio de Janeiro 2007

The **Internet Governance Forum** (**IGF**) is a multi-stakeholder forum for policy dialogue on issues of Internet governance. The establishment of the IGF was formally announced by the United Nations Secretary-General in July 2006 and it was first convened in October / November 2006.

Structure and Function

The formation of the Internet Governance Forum was first recommended in the report of the Working Group on Internet Governance following a series of open consultations. This report was one of the inputs to the second phase of the World Summit on the Information Society in Tunis in 2005, which formally called for the creation of the IGF and set out its mandate.

Following an open consultation meeting called in February 2006, the UN Secretary-General established an Advisory Group, the MAG, and a Secretariat as the main institutional bodies of the IGF.

These organizational divisions should not be considered concrete since the organizational structures will continue to be adjusted and to be changed until they fit into the needs of the members.

Multistakeholder Advisory Group - MAG

The Advisory Group, now referred to as the MAG (Multistakeholder Advisory Group), was set up by the former Secretary General of the United Nations, Mr Kofi Annan on May 17, 2006. The MAG was originally made up of 46 Members from international governments, the commercial private sector and public civil society, including academic and technical communities, and was chaired by Nitin Desai- the Secretary-General's Special Adviser for the World Summit on the Information Society. All stakeholders participate as equals. The purpose for which the MAG was set up was to assist the Secretary General in convening the Internet Governance Forum. On August 20, 2007, the mandate of the MAG was renewed with a new structure of 47 members, and a Co-Chairmanship by Nitin Desai, and Brazilian diplomat Hadil da Rocha Vianna. The mandate of the MAG was further extended on April 30, 2008 with a renewed one third of its members within each stakeholder group and Nitin Desai serving as the sole Chairman. The MAG meet three times each year - in February, May and September. All three meetings take place in Geneva at the Palais des Nations and they are preceded by open consultations meeting.

The details on MAG's operating principles and selection criteria are contained in the summary report of its February meeting available at this link.

On August 22, 2008, the United Nations Office in Geneva renewed the membership of MAG to prepare for the Internet Governance Forum Meeting in Hyderabad, India. There were a total of 50 members, among them 17 new appointed members, which represents 1/3 of its membership. Nitin Desai continues to be the Chairman for the Advisory Group. (Source: UN Department of Public Information, United Nations Office in Genev. Accessed online at:

- Actual List of Members
- MAG Meetings

Secretariat

The Secretariat, based in the United Nations Office in Geneva, assists and coordinates the work of the MAG, Multistakeholder Advisory Group. The Secretariat is headed by Markus Kummer with the designation of Executive Coordinator and Chengetai Masango is Programme and Technology Manager. The Secretariat also hosts fellowships. Markus Kummer has also been involved with the WGIG as its Executive Coordinator of the Secretariat.

History and Development of the Internet Governance Forum

WSIS Follow Ups

The IGF is considered an important development of the World Summit on Information Technology (WSIS). This important outcome was reaffirmed by paragraphs 37 and 38 of the Tunis 2005 Commitment. Paragraph 37 states that *"...goals can be accomplished through the involvement, cooperation and partnership of governments and other stakeholders, i.e. the private sector, civil society and international organizations, and that international cooperation and solidarity at all levels are indispensable if the fruits of the Information Society are to benefit all."* Corollary to this commitment, paragraph 38 states, too, that all efforts from here on *"should not stop with the conclusion of the Summit…emergence of the global Information Society to which we all contribute provides increasing opportunities for all our peoples and for an inclusive global community…we must harness these opportunities today and support their further development and progress."*

The Tunis Summit of 2005 made significant headway when the mandate of the IGF was formulated. In paragraph 72 of the Tunis Agenda, the UN Secretary-General was asked to convene a meeting with regards to the new multi-stakeholder forum, otherwise known as the IGF. In this mandate, different stakeholders are encouraged to strengthen engagement, particularly those from developing countries. In paragraph 72(h), the mandate focused on capacity-building for developing countries and the drawing out of local resources. This particular effort, for instance, has been reinforced through *Diplo Foundation's* Internet Governance Capacity Building Programme (IGCBP) that allowed participants from different regions to benefit from valuable resources with the help of regional experts in IG.

The involvement of different stakeholders in the policy framework of the IGF is a re-affirmation of commitment as per paragraph 39 of the Tunis Commitment. In this particular context, there is a deep resolve to *"...develop and implement an effective and sustainable response to the challenges and opportunities of building a truly global Information Society that benefits all our peoples."* During the OECD Civil Society-Organized Labour Forum held last June 16, 2008, in Seoul, Korea, Ambassador David A. Gross of the US Department of State talked about the transformation of the Internet in the social lives of people. He believed that this transformation made an impact in the free flow of information that politically drives challenges. Ambassador Gross commented on the 2005 WSIS because of the powerful language used on paragraph 4 of the Tunis agenda that reiterated on openness.

Formation of the IGF

A multi-stakeholder's approach was reiterated in the coordination of international activities for the IGF. This adaptation was set from paragraphs 29 to 35 of the Tunis agenda. These stakeholders were defined as coming from governments, the private technical and economic sector, civil society, intergovernmental organizations, and

international organizations. In paragraph 32, the UN Secretary-General was commended for his efforts in establishing the Working Group on Internet Governance (WGIG).

The suggested need of an organization like the IGF was first pointed out in the WGIG Report. After reaching a clear consensus among its members the WGIG proposed in paragraph 40 of the Report that:

"(t)he WGIG identified a vacuum within the context of existing structures, since there is no global multi-stakeholder forum to address Internet-related public policy issues. It came to the conclusion that there would be merit in creating such a space for dialogue among all stakeholders. This space could address these issues, as well as emerging issues, that are cross-cutting and multidimensional and that either affect more than one institution, are not dealt with by any institution or are not addressed in a coordinated manner".

The IGF was one of four proposals made in the report.

The idea of the Forum was also proposed by Argentina, as stated in its proposal made during the last Prepcom 3 in Tunis:

"(t)In order to strengthen the global multistakeholder interaction and cooperation on public policy issues and developmental aspects relating to Internet governance we propose a forum. This forum should not replace existing mechanisms or institutions but should build on the existing structures on Internet governance, should contribute to the sustainability, stability and robustness of the Internet by addressing appropriately public policy issues that are not otherwise being adequately addressed excluding any involvement in the day to day operation of the Internet. It should be constituted as a neutral, non-duplicative and non-binding process to facilitate the exchange of information and best practices and to identify issues and make known its findings, to enhance awareness and build consensus and engagement. Recognizing the rapid development of technology and institutions, we propose that the forum mechanism periodically be reviewed to determine the need for its continuation."

The convening of the IGF was announced on 18 July 2006, with the inaugural meeting of the Forum being held in Athens, Greece from 30 October to 2 November 2006.

Consultations

There were two rounds of consultations with regards to the convening of the first IGF:

16 – 17 of February 2006 – The first round of consultations was held in Geneva. The transcripts of the two-day consultations are available in the IGF site.

19 May 2006 – The second round of consultations was open to all stakeholders and was coordinated for the preparations of the inaugural IGF meeting. The meeting chairman

was *Nitin Desai* who is the United Nations Secretary-General's Special Adviser for Internet Governance.

The Second Meeting of the IGF

Consultations held in Geneva last May 23, 2007 were open to all stakeholders. This consultation was part of a cluster of related events of the WSIS that took place last 15-25 of May 2007. An advisory group was also facilitated for the IGF meeting in Rio de Janeiro, Brazil. The IGF open Consultations held last 3 September 2007 was held in Geneva.

For further information, a summary of the IGF consultations and meetings can be found below:

Date	Event
16–18 November 2005	Second Phase of the WSIS in Tunis
16 – 17 February 2006	First Round of Consultations
2 March 2006	Establishment of the IGF Secretariat
19 May 2006	Second Round of Consultations
22 – 23 May 2006	Establishment and First Meeting of the IGF Advisory Group
18 July 2006	Convening of the IGF
7 – 8 September 2006	Second Meeting of the IGF Advisory Group
30 October – 2 November 2006	Inaugural Meeting of the IGF in Athens
12–15 November 2007	Second Meeting of the IGF in Rio de Janeiro, Brazil

13 May 2008	Open Consultations
14–15 May 2008	Meeting of the IGF Multistakeholder Advisory Group(**MAG**)
3–6 December 2008	Third meeting of the IGF in Hyderabad, India
15–18 November 2009	Fourth Meeting of the IGF in Sharm El Shiekh, Egypt
14–17 September 2010	Fifth Meeting of the IGF in Vilnius, Lithuania

The government of Egypt offered to host the 2009 IGF meeting, while the governments of Lithuania and Azerbaijan made a bid for the 2010 meeting.

Mandate and Outcome

The mandate of the IGF is principally that of a discussion forum for facilitating dialogue between the participants. The IGF may *"identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations,"* but does not have any direct decision-making authority.

Activities at the IGF

The following are the activities that take place during the IGF: Workshops, Best Practice Forums, Open Forums and meetings of the Dynamic Coalitions.

The main themes of IGF are: openness, security, diversity and access. A new theme was introduced in IGF Brazil: critical Internet resources being one of the most debatable topics in the IG field at the moment.

Dynamic Coalitions

The most tangible result of the first IGF in Athens is the establishment of a number of so-called *Dynamic Coalitions*. These coalitions are relatively informal, issue-specific groups consisting of stakeholders that are interested in the particular issue.

Most coalitions allow participation of anyone interested in contributing. Thus, these groups gather not only academics and representatives of governments, but also members of the civil society interested in participating on the debates and engaged in the coalition's works.

So far, the following Dynamic Coalitions were brought to the attention of the IGF Secretariat:

- The StopSpamAlliance
- Dynamic Coalition on Privacy
- The IGF Dynamic Coalition on Open Standards (IGF DCOS)
- The Dynamic Coalition on Access and Connectivity for Remote, Rural and Dispersed Communities
- Dynamic Coalition on the Internet Bill of Rights
- Dynamic Coalition for Linguistic Diversity
- A2K@IGF Dynamic Coalition
- Freedom of Expression and Freedom of the Media on the Internet (FOEonline)
- Online Collaboration Dynamic Coalition
- Gender and Internet Governance (GIG)
- Framework of Principles for the Internet
- Dynamic Coalition on Child Online Safety
- Dynamic Coalition on "Accessibility and Disability"
- Dynamic Coalition for Online Education

Active Dynamic Coalitions

Workshops

In 2007, IGF hosted a number of workshops which attracted great interest with the public. In particular, the theme of child protection was one of the topics that increased the engagement of the participants in the events.

For 2008 the IGF page stipulates that workshops can be proposed on the draft main session headings:

```
  * Universalization of the Internet - How to reach the next billion
(Expanding the Internet)
  * Low cost sustainable access
  * Multilingualization
  * Implications for development policy
  * Managing the Internet (Using the Internet)
  * Critical Internet resources
  * Arrangements for Internet governance
  * Global cooperation for Internet security and stability
  * Taking stock and the way forward
  * Emerging issues
```

The following workshops have been proposed as of 15 May 2008, according to the Workshop page . These proposals will be reviewed and an attempt will be made to merge propositions into a manageable number of workshops.

Number Proposed	Workshop Theme
15	Access
9	Diversity
15	Openness
21	Security
13	Critical Internet Resources
9	Development
6	Capacity Building
17	Other

I IGF Athens 2006

The host webpage brings interesting information about the evolution of the first IGF.

II IGF Rio 2007

There were 84 events happening in parallel to the main sessions, organized under the 5 main themes: (i) critical Internet resources; (ii) access; (iii) diversity; (iv) openness and (v) security. There were 36 workshops, 23 best practices forums, 11 dynamic coalitions meetings, 8 open forums and 6 events covering other issues (like the Giganet Symposium)

The host webpage keeps video and audio records from main sessions and some parallel events such as workshops, best practices and open forums, as well as the tool for translation into Arabic.

Regarding the participation by region, around 35% of the attendees came from the Latin America and Caribbean of which 29% were from the host country (Brazil).

There are also some interesting statistics such as:

Region	Participation
Latin America and Caribbean	35%
Western Europe	20%
North America	13%
Asia	13%
Africa	10%
Eastern Europe	7%
Oceania	2%

Main sessions

The main sessions were developed according to the five themes chosen for this year: Critical Internet Resources, Access, Diversity, Openness and Security.

Please see below the summary of the main sessions:

Opening Ceremony/Opening Session

The multistakeholder approach was highlighted by many speakers and panelists during the Opening Session, including the message from the UN Secretary-General Ban Ki-Moon, which was read by the UN Under-Secretary-General for Economic and Social Affairs, M. Sha Zukang.

M. Ban Ki-Moon assured that it is not a UN goal to take over Internet Governance but the UN will offer an opportunity to bring people together, with the same interest, in a global reach.

M. Sha Zukang concludes that the IGF was a unique experience because *"it brings together people who normally do not meet under the same roof."*

"Development" was a key discussion during the IGF Rio Meeting. It will still be an important aspect for discussion, together with the issue of bridging the digital divide - a key element of discussion for the IGF Hyderabad and reflects the theme of the IGF Hyderabad which is "Internet for All."

The nature and prospective of the IGF were also discussed, as the Chairman properly summarizes:

"Several participants underlined that the IGF was not only a space for dialogue, but also a medium that should encourage fundamental change at the local level to empower communities, build capacity and skills enable the Internet's expansion, thereby contributing to economic and social development."

Critical Internet Resources

This is a new session that was introduced during the IGF Rio Meeting. Basically, it covered some issues pertaining to the infrastructure of the Internet. ICANN discussions were not missed, as well as the role of governments in shaping policies.

Access

The issue of "access" is more on how to get the billion of users around the world to go online in the next years to come. Such initiatives to this cause are reminiscent of pilot projects in Africa wherein laptops were given to children under an open source software agreement.

Diversity

The issue of "diversity" calls for multilingualism in the Net. Such promotion on multilingualism would increase users whose main language is not English. In order to open the Net to a diverse population, international domain names (IDN) were added to facilitate the language needs of other users.

Openness

The strong support on closed software has not been favorable to some people. This is because there were long-lasting agreements between governments and large software companies. Such actions were considered critical, as it binds different entities to proprietary or closed source technologies. Many believed that the shift from closed to open software can only happen with the full-scale participation of both the private and public sectors. As such, many people fear the turning of the Internet into a "private" network if there is much insistence on the use of closed technologies.

Talks on open standards, open architecture and open software are clear indicators of what the issue on openness is all about.

Read this literature entitled "Free Culture" by Lawrence Lessig to know more on "Openness on the Internet."

Security Issues

The question of Internet Security is one of the most important debate in the Information Society. Internet is becoming an important communication and business tool, as such, that the question of security comes as a cross-cutting issue to be addressed in all its dimension. As indicated by Michael Harrop, Rapporteur SG 17 Q4, Communications Security Project in 2006, *"without effective security, all systems and processes that rely on electronic communications are at risk and, as a consequence, large numbers of resources are now devoted to countering threats, protecting systems and recovering from successful attacks."* The Rio de Janeiro Meeting mentioned that *"...achieving the Internet's full potential to support commercial and social relationships required an environment that promoted and ensured users' trust and confidence and provided a stable and secure platform."*

Cyber-security, in this case, focused heavily on child protection, particularly on child pornography. Participants gathered were called to seek ways to harmonize legislative agendas to counter-act such crimes. This was a call of legislation between countries that can work together in order to enforce laws that would protect children. As such that some laws are not applicable online, this call also promoted formulation of legislation that would be applicable in the online or virtual world.

Internet Security has been mentioned in the Substantive Agenda of the Rio de Janeiro Meeting. It was also present in the Agenda of the Athens Meeting. Even before the Athens Meeting, Internet Security was mentioned at the Tunis WSIS under "Building Confidence and Security in the Use of ICT's." At the coming Hyderabad Meeting in December 2008, two panels will again discuss questions related to Internet Security. This gives an idea on how important the question has been in each of the IGF meetings so far.

Internet Security issues can be folded under the following:

- secure telecommunication which deals most with the security of telecommunication infrastructure
- cyber-security as Internet users deal with it in their daily operations and use of the Internet
- identity theft
- children pornography
- hacking and other virus and cyber threats (scams, spams, etc.)
- cyber-terrorism

Internet Security on the Athens Agenda

The International Telecommunication Union (ITU) is at the forefront of contributors to the field of Telecommunication Security. At the Athens meeting, ITU mentioned the major contributions made in this domain by International organizations. ITU took the necessary steps to set up a number of initiatives that were presented at the Athens meeting. It presented a telecommunication security guideline and set up the road map towards Internet Security. The question of security of telecommunication was somehow dominant at the Athens meeting.

ITU mentioned the difficulty of experts in the field. One of the difficulties mentioned was related to the question of standardisation - as many international organizations were developing domain initiatives at the same time.

As a follow-up activity of the WSIS Conference, a number of ITU study groups have been assigned tasks related to Internet Security. At the Athens Meeting, findings of these study groups were presented to address diverse Internet security questions such as:

- Telecommunication management
- Protection against electromagnetic environment effects
- Outside Plant and related indoor installations
- Security, languages and telecommunication software
- Mobile Telecommunications Networks

Internet Security on the Rio de Janeiro Agenda

At the Rio de Janeiro meeting, a whole session was dedicated to the question of Internet security, emphasizing the importance of this question nowadays, as well as the threats, that users are facing more and more in their daily operations over the Internet. Internet Security questions put on the agenda at Rio were related to:

- cybercrime
- cyber-terrorism
- protection of individuals and automatic processing of personal data
- action against trafficking in human beings
- protection of children against sexual exploitation and sexual abuse

The Rio de Janeiro meeting called for international cooperation and coordinated action to counter cybercrime because of its trans-national dimension. Recommendations were forwarded towards the direction of responsibility of governments in order to raise awareness among Internet users and in the direction of ICANN because of the responsibility it has for the Domain Name System. It is required of ICANN since it accepts responsibility for controlling illegal online content for the protection of children from Internet pornography.

Taking Stock and the Way Forward

Emerging Issues

This session aims to identify key issues in Internet Governance that should be addressed in the Forum. The first obstacle was to filter some themes, as there is a variety of interests to be held in such a generic target. There were four themes proposed:

(i) **demand and supply side initiatives** (by Robert Pepper). He brought into debate the economic concept of demand and supply applied to Internet Governance. On the demand side, there were interesting proposals, such as the need for educating through capacity-building Internet users, the ability of people controlling their web ID (part of educating the usage in Internet), local content in local languages (enforcing local community) and improving public policies (but not over regulating, such as prohibiting or limiting access to VoIP, which can suppress the demand). On the supply side, there were the common concern of extending Internet users/access, but also considering *"the opportunities created by the release of spectrum through the switch to digital broadcasting were highlighted. Some speakers suggested that such spectrum could be used to support new broadband networks and support new investment and innovative services, while others held the view that this would not be a sustainable solution."*

(ii) **social, cultural and political issues of Web 2.0** (by Andrew Keen);

(iii) **access** (particularly in Africa, by Nii Quaynor) and

(iv) **innovation, research and development** (by Robert Kahn).

Another challenge was to discuss emerging issues in a global forum with different perspectives, for example, developed and developing countries realities; democratic and non-democratic political regimes; and etc.

III IGF Hyderabad 2008

The third meeting of the IGF was held in Hyderabad, India. The over-all theme for the meeting was "Internet for All." The chairman's summary can be accessed via the official IGF website.

In terms of attendance, there were 1280 participants from 94 countries. The actual breakdown of participants by region can be found here.

Renewal of the Multistakeholder Advisory Group (MAG)

Stakeholders from different sectors - government, civil society, private, academe and technical communities - were invited to submit proposals/nominations for new MAG members. The mandate behind the rotation of its members are based on recommendations

from different sectors. The official IGF website carries the list of updated MAG members.

Remote Participation in the IGF 2008

The Remote Participation Working Group (RPWG) has been working closely with the IGF Secretariat for allowing remote participants across the globe to interact in the meeting. There were 522 remote participants from around the world who joined the main sessions and workshops.

The entire meeting in Hyderabad was webcast in real-time using high quality video, audio streaming and live chat.

Remote Hubs were also introduced with remote moderators leading the discussions in their region. Most of the hubs were able to discuss pertinent local and domestic Internet Governance issues. The Remote Hubs were found in Buenos Aires, Argentina, Belgrade, Serbia, São Paulo (Brazil), Pune (India), Lahore (Pakistan), Bogotà (Colombia), Barcelona and Madrid (Spain).

The platform used for remote participation in Hyderabad was DimDim.

IV IGF Sharm El Sheikh 2009

Egypt hosted the fourth IGF meeting in Sharm el Sheikh from 15–18 November 2009 in Sharm El Sheikh. “Internet Governance – Creating Opportunities for all” is the overall title of the meeting. It marks the beginning of a new multi-stakeholder process.

The main sessions on the agenda points are Managing Critical Internet Resources; Security, Openness and Privacy; Access; Diversity; Internet governance in the Light of WSIS Principles; Taking Stock and the Way forward – on the Desirability of the Continuation of the Forum; and Emerging Issues - Impact of Social Networks.

One key focus of IGF 2009 is encouraging youth participation towards Internet Governance issues.

Remote Participation in the IGF 2009

Following the success of remote participation in the IGF Hyderabad, the Remote Participation Working Group (RPWG) has come up with improved guidelines on intervention for the training of remote moderators. Webex was also used as the platform for this year's remote participation. There are 11 registered remote hubs for this year's meeting and the complete list can be found in the official IGF website.

Chapter 4

InterNIC and Internet Watch Foundation

InterNIC

The **Internet Network Information Center**, known as **InterNIC**, was the Internet governing body primarily responsible for domain name and IP address allocations until September 18, 1998 when this role was assumed by the Internet Corporation for Assigned Names and Numbers (ICANN). It was accessed through the domain name **internic.net**, with email, FTP and World Wide Web services run by Network Solutions, Inc and AT&T.

Term

InterNIC is a registered service mark of the U.S. Department of Commerce. The use of the term is licensed to the Internet Corporation for Assigned Names and Numbers (ICANN).

History

The first central authority to coordinate the operation of the network was the Network Information Center (NIC) at the Stanford Research Institute (SRI) in Menlo Park, California. In 1972, management of network resources was transferred to the newly created Internet Assigned Numbers Authority (IANA). Jon Postel fulfilled the role of manager of IANA, in addition to his role as the RFC Editor, until his death in 1998.

On the ARPANET, hosts were given names to be used in place of numeric addresses and a HOSTS.TXT file was distributed by SRI International and manually installed on each host on the network to provide a mapping between these names and their corresponding network address. As the network grew, this became increasingly cumbersome. A technical solution came in the form of the Domain Name System, created by Paul Mockapetris. The Defense Data Network Network Information Center (DDN-NIC) at SRI handled all registration services, including the top-level domains `mil`, `gov`, `edu`, `org`, `net`, `com` and `us`. DDN-NIC also performed root nameserver administration and Internet number assignments under a United States Department of Defense contract. In 1991, the Defense Information Systems Agency (DISA) awarded the administration and maintenance of DDN-NIC, which had been up until this point under the management of

SRI for many years, to Government Systems, Inc. which subcontracted it to the small private-sector firm Network Solutions, Inc.

Up to this time, most of the growth of the Internet was in the non-military sector. Therefore, it was decided that the Department of Defense would no longer fund registration services outside of the `mil` domain. In 1993, the National Science Foundation of the United States, after a competitive bidding process in 1992, created the Internet Network Information Center, known as *InterNIC*, to manage the allocations of addresses and awarded the contract to three organizations. Registration services were to be provided by Network Solutions, directory and database services were to be run by AT&T, and information services by General Atomics. Later, General Atomics was disqualified from the contract after a review found their services not conforming to the standards of its contract. General Atomics' InterNIC functions were assumed by AT&T. AT&T discontinued InterNIC services after their contract expired.

In 1998 both IANA and InterNIC were reorganized under the control of ICANN, a California non-profit corporation contracted by the US Department of Commerce to manage a number of Internet-related tasks. The role of operating the DNS system was privatized, and opened up to competition, while the central management of name allocations would be awarded on a contract tender basis.

Domain name restrictions

Via internic.net, domain names were distributed through an automated system. Beginning in 1996, Network Solutions began restricting the distribution of domain names containing a number of words on a "restricted list" through an automated filter. The filter is known to have rejected domain names containing the "least agreeable words in the English language" Applicants whose domain names were rejected would receive a form email containing the notice: "Network Solutions has a right founded in the First Amendment to the U.S. Constitution to refuse to register, and thereby publish, on the Internet registry of domain names words that it deems to be inappropriate."

This filter came under heavy scrutiny, as legitimate domain names such as "shitakemushrooms.com" would be rejected, but the domain name "shit.com" was active, as it had been registered before 1996. Network Solutions eventually allowed domain names containing the words on a case-by-case basis, after manually reviewing the names for obscene intent. This profanity filter was never enforced by the government and its use was not continued by ICANN when it took over governance of the distribution of domain names to the public.

Internet Watch Foundation

Internet Watch Foundation

Type	Registered charity
Founded	1996
Employees	14 (2007)

The **Internet Watch Foundation (IWF)** is a non-governmental charitable body based in the United Kingdom. It offers an online service for the public and IT professionals to report content on the Internet that it considers to be "potentially illegal". As part of its function, the IWF produces a blacklist of Internet sites and content that it deems to be in contravention/potentially in contravention to UK laws. Since 2010, blocking Internet users from accessing the content on this list is mandatory for all UK based ISPs that want to be eligible for contracts with government agencies and other public bodies.

The IWF operates in informal partnership with the police, government, public and Internet service providers. Originally formed to police suspected child pornography online, the IWF's remit was later expanded to cover racist and criminally obscene material.

The IWF is an incorporated charity, limited by guarantee, and largely funded by voluntary contributions from UK communications service providers, including ISPs, mobile phone operators, Internet trade associations, search engines, hardware manufacturers, and software providers. It also receives funding from the Association for Payment Clearing Services and the European Union.

The IWF is governed by a Board of Trustees which consists of an independent chair, six non-industry representatives, and three industry representatives. The Board monitors and reviews IWF's remit, strategy, policy and budget to enable the IWF to achieve its objectives. The IWF operates from offices in Oakington, near Cambridge.

History

Background

During 1996 the Metropolitan Police told the Internet Service Providers Association (ISPA) that the content carried by some of the newsgroups made available by them was illegal, that they considered the Internet Service Providers (ISPs) involved to be publishers of that material, and that they were therefore breaking the law. In August 1996, Chief Inspector Stephen French, of the Metropolitan Police Clubs & Vice Unit, sent an open letter to the ISPA, requesting that they ban access to a list of 132 newsgroups, many of which were deemed to contain pornographic images or explicit text.

This list is not exhaustive and we are looking to you to monitor your newsgroups identifying and taking necessary action against those others found to contain such material. As you will be aware the publication of obscene articles is an offence. This list is only the starting point and we hope, with the co-operation and assistance of the industry and your trade organisations, to be moving quickly towards the eradication of this type of newsgroup from the Internet ... We are very anxious that all service providers should be taking positive action now, whether or not they are members of a trade association. We trust that with your co-operation and self regulation it will not be necessary for us to move to an enforcement policy.
—Chief Inspector Stephen French, quoted in *Web Control*

The list was arranged so that the first section consisted of unambiguously titled paedophile newsgroups, then continued with other kinds of groups which the police wanted to restrict access to, including *alt.binaries.pictures.erotica.cheerleaders* and *alt.binaries.pictures.erotic.centerfolds*.

Although this action had taken place without any prior debate in Parliament or elsewhere, the police, who appeared to be doing their best to create and not simply to enforce the law, were not acting entirely on their own initiative. Alan Travis, Home Affairs editor of the newspaper *The Guardian*, explained in his book "Bound and Gagged" that Ian Taylor, the Conservative Science and Industry Minister at the time, had underlined an explicit threat to ISPs that if they did not stop carrying the newsgroups in question, the police would act against any company that provided their users with "pornographic or violent material". Taylor went on to make it clear that there would be calls for legislation to regulate all aspects of the Internet unless service providers were seen to wholeheartedly "responsible self-regulation".

Demon Internet regarded the police request as "unacceptable censorship"; however, its attitude annoyed ISPA chairman Shez Hamill, who said:

We are being portrayed as a bunch of porn merchants. This is an image we need to change. Many of our members have already acted to take away the worst of the Internet.

But Demon have taken every opportunity to stand alone in this regard. They do not like the concept of our organisation.
—*Observer*, 25 August 1996

Following this, a tabloid-style exposé of ISP Demon Internet appeared in the *Observer* newspaper, which alleged that Clive Feather (a director of Demon) "provides paedophiles with access to thousands of photographs of children being sexually abused".

During the summer and autumn of 1996 the UK police made it known that they were planning to raid an ISP with the aim of launching a test case regarding the publication of obscene material over the Internet. The direct result of the campaign of threats and pressure was the establishment of the Internet Watch Foundation (initially known as the Safety Net Foundation) in September 1996.

Foundation of IWF

Facilitated by the Department of Trade & Industry (DTI), discussions were held between certain ISPs, the Metropolitan Police, the Home Office, and a body called the "Safety Net Foundation" (formed by the Dawe Charitable Trust). This resulted in the "R3 Safety Net Agreement", where "R3" referred to the triple approach of rating, reporting, and responsibility. In September 1996, this agreement was made between the ISPA, LINX, and the Safety Net Foundation, which was subsequently renamed the Internet Watch Foundation. The agreement set requirements for associated ISPs regarding identifiability and traceability of Internet users; ISPs had to cooperate with the IWF to identify providers of illegal content and facilitate easier traceability.

Demon Internet was a driving force behind the IWF's creation, and one of its employees, Clive Feather, became the IWF's first chair of the Funding Board and solicitor Mark Stephens the First Chair of the IWF's Policy Board. The Policy Board developed codes, guidance, operational oversight and a hotline for reporting content.

The Funding Board, made up of industry representatives and Chair of Policy Board, provided the wherewithall for the IWF's day to day activities as set down and required by the Policy Board.

After 3 years of operation, the IWF was reviewed for the DTI and the Home Office by consultants KPMG and Denton Hall. Their report was delivered in October 1999 and resulted in a number of changes being made to the role and structure of the organisation, and it was relaunched in early 2000, endorsed by the government and the DTI, which played a "facilitating role in its creation", according to a DTI spokesman.

At the time, Patricia Hewitt, then Minister for E-Commerce, said: "The Internet Watch Foundation plays a vital role in combating criminal material on the Net." To counter accusations that the IWF was biased in favour of the ISPs, a new independent chairman was appointed, Roger Darlington, former head of research at the Communication Workers Union.

The website

The IWF's website offers a web-based government-endorsed method for reporting suspect online content and remains the only such operation in the United Kingdom. It acts as a Relevant Authority in accordance with the Memorandum of Understanding concerning Section 46 of the Sexual Offences Act 2003 (meaning that its analysts will not be prosecuted for looking at illegal content in the course of their duties). Reports can be submitted anonymously. The IWF aims to minimise the availability of potentially illegal Internet content, specifically:

- Indecent images of under-18s hosted anywhere in the world;
- criminally obscene content hosted in the UK, or anywhere in the world if uploaded by a British citizen (under the Obscene Publications Acts);
- *incitement to racial hatred content hosted in the UK*

However, almost the whole of the IWF site is concerned with suspected child pornography with little mention of the rest of their remit (racial hatred and criminally obscene material). Images judged by the IWF to be child pornography are blocked, whilst other possibly illegal content is reported to the police for further action.

The Government claimed that they would also be handling images of adult "extreme pornography" which are now illegal for UK citizens to possess as of 26 January 2009. The IWF now includes "extreme pornography" as an example under "criminally obscene content", meaning that they will report material hosted in the UK, or uploaded by a British citizen, but has stated that it has no plans to block any such material, or handle sites hosted outside on the UK.

The IWF states that it works in partnership with UK Government departments such as the Home Office and the Department for Business, Enterprise and Regulatory Reform to influence initiatives and programmes developed to combat online abuse.

They are funded by the European Union and the online industry. This includes Internet service providers, mobile operators and manufacturers, content service providers, telecommunications and filtering companies, search providers and the financial sector as well as blue-chip and other organisations who support the IWF for corporate social responsibility reasons.

Through their "Hotline" reporting system, the organisation helps ISPs to combat abuse of their services through a "notice and take down" service by alerting them to any potentially illegal content within their remit on their systems and simultaneously invites the police to investigate the publisher.

The IWF has connections with the Virtual Global Taskforce, the Serious Organised Crime Agency and the Child Exploitation and Online Protection Centre.

Management

Peter Robbins OBE, QPM is IWF Chief Executive

Sarah Robertson is IWF Director of Communications

Fred Langford is IWF Director of Technology and Content

Cross-border aspects

Previously, the IWF passed on notifications of suspected child pornography hosted on non-UK servers to the UK National Criminal Intelligence Service which in turn forwards it to Interpol or the relevant foreign police authority. It now works with the Serious Organised Crime Agency instead. The IWF does not, however, pass on notifications of other types of illegal content hosted outside the UK.

Blacklist

The IWF compiles and maintains a blacklist, mainly of what it considers child pornography URLs, from which 95% of commercial Internet customers in the UK are filtered. A staff of four police-trained analysts are responsible for this work, and the director of the service has claimed that the analysts are capable of adding an average of 65-80 new URLs to the list each week, and act on reports received from the public rather than pursuing investigative research.

Between 2004 and 2006, BT Group introduced its Cleanfeed technology which was then used by 80% of internet service providers. BT spokesman Jon Carter described Cleanfeed's function as "to block access to illegal Web sites that are listed by the Internet Watch Foundation", and described it as essentially a server hosting a filter that checked requested URLs for Web sites on the IWF list, and returning an error message of "Web site not found" for positive matches.

In 2006, Home Office minister Alan Campbell pledged that all ISPs would block access to child abuse websites by the end of 2007. By the middle of 2006 the government reported that 90% of domestic broadband connections were either currently blocking or had plans to by the end of the year. The target for 100% coverage was set for the end of 2007, however in the middle of 2008 it stood at 95%. In February 2009, the Government said that it is looking at ways to cover the final 5%. In an interview in March 2009, a Home Office spokesperson mistakenly thought that the IWF deleted illegal content, and didn't look at the content they rate.

Although the IWF's blacklist causes content to be censored even if the content has not been found to be illegal by a court of law, IWF Director of Communications Sarah Robertson claimed, on 8 December 2008, that the IWF is opposed to the censorship of legal content.

In March 2009 a Home Office spokesperson said that ISPs were being pressured to sign up to the IWF's blacklist in order to block child pornography websites and said that there was no alternative to using the IWF's blacklist. One of the ISPs which refused to subscribe to the blacklist, Zen Internet, has said that it has "concerns over its effectiveness".

As of 2009, the blacklist was said to contain about 450 URLs. A 2009 study by researcher Richard Clayton at the University of Cambridge found that about a quarter of them were on (otherwise) legitimate free file hosting services, among them RapidShare, Megaupload, SendSpace and Zshare. According to the *Times*, the list contained "between 500 and 800 websites" as of March 2010, and was updated two times per day.

It appears, around July/August 2010, Megaupload, and Megavideo were added to the blacklist again. Access to these sites via some exchange routers used by O2 broadband is restricted. A few members appear to be blocked with no way of appealing this decision.

Incidents

Sex stories

On 26 July 2007, UK tabloid newspaper *The Daily Star* reported that it had discovered an online text story about British pop group Girls Aloud that it described as "a chilling story detailing each singer's gory death in scenes that could be straight out of a horror movie", characterizing its author as "a vile internet psycho" and "a cyber-sicko". The news story said that *The Daily Star* had reported the content of the hosting website, "Kristen Archives" (a subsite of the ASSTR archive), to the IWF, and that the IWF had traced the site to the US. It also claimed that Interpol had been notified to help track down the site's operators and the writer of the story. An IWF spokesperson was reported as saying that since the site was hosted in the US, it fell outside the organization's remit, but that they were aware of the site. The spokesperson added that the site also contained "child abuse fantasy stories" and that they had passed on details of it to the British police.

Although the story, entitled "Girls (Scream) Aloud", had been published on a US website, British police carried out the investigation because the alleged author was identified as living in the UK. Although he had submitted the story under a pseudonym, he included an email address which was reportedly traced. Officers from Scotland Yard's Obscene Publications Unit decided to take action over the story after consulting the Crown Prosecution Service (CPS), and on 25 September 2008 it was announced that the author, Darryn Walker, was to be prosecuted for the online publication of material that the police and the CPS believed was obscene. It was the first such prosecution for written material in nearly two decades, and was expected to have a significant impact on the future regulation of the Internet in the UK.

Walker appeared in court on 22 October 2008 to face charges of "publishing an obscene article contrary to Section 2(1) of the Obscene Publications Act 1959". He was granted unconditional bail, and his case was set for trial on 16 March 2009. However, at a

directions hearing in January, the defendant made it known that given the seriousness of the case he would be represented by a QC (Queen's Counsel), following which the Crown Prosecution Service gave notice of its intention to similarly employ a QC, and the trial date was put back to 29 June 2009, where the defendant was found not guilty, and cleared of all charges of obscenity.

Wayback Machine

On 14 January 2009 some UK users reported that all of the 85 billion pages of the Internet Archive (Wayback Machine) had been blocked, in spite of the fact that the IWF's policy is to try to only censor the exact webpage in question and not the whole domain. According to IWF chief executive Peter Robbins this happened due to a "technical hitch". Because the Internet Archive's web site contained URLs on the IWF's blacklist, requests sent there from the ISP Demon Internet carried a particular header, which clashed with the Internet Archive's internal mechanism to convert web links when serving archived versions of web pages. The actual blocked URL which had caused the incident never became publicly known.

Criticism

Charity status

In February 2009 a Yorkshire-based software developer lodged a formal complaint regarding the IWF status as a charity with the Charity Commission, in which he pointed out that "regulating the worst of the internet" was "not really a charitable purpose", and that the IWF existed mainly to serve the interests of ISPs subscribing to it rather than the public. An IWF spokesperson said that the IWF had attained charitable status in 2004 "in order to subject itself to more robust governance requirements and the higher levels of scrutiny and accountability which charity law, alongside company law, brings with it". The IWF is listed by fakecharities.org, "a directory of those so-called charities that receive substantial funding from either the UK or EU governments". It has also been termed a quango by critics, implying poor management and lack of accountability.

False positives

Following the IWF's blacklisting of the article, the organisation's operating habits came under scrutiny. J.R. Raphael of PC World stated that the incident had raised serious free-speech issues, and that it was alarming that one non-governmental organisation was ultimately acting as the "morality police" for about 95% of UK's Internet users. Frank Fisher of *The Guardian* criticized the IWF for secretiveness and lack of legal authority, among other things, and noted that the blacklist could contain anything and that the visitor of a blocked address may not know if their browsing is being censored.

Forced adoption

The government believes that a self-regulatory system is the best solution, and the Metropolitan Police also believe that working with ISPs, rather than trying to force them via legislation, is the way forward. The IWF has a blacklist of URLs which is available to ISPs, but ISPs are not forced to subscribe to it. However, ISPs may feel inclined or even forced to join (and contribute) to the IWF's activities as a failure to do so may harm their reputation as responsible providers. Subscribing to the IWF may also be seen as a marketing tool by ISPs.

Legality

As a "self-appointed, self-regulated internet watchdog, which views user-submitted content and compiles a list of websites that it deems to contain illegal images" there have been questions raised regarding the legality of their viewing content that would normally constitute a criminal offense.

Secrecy

The IWF has been criticized for blacklisting legal content and for not telling websites that they are being blocked and also for not making their blocked website list public.

Technical issues

In addition to introducing performance problems the blacklisting of sites may be concealed by generic HTTP 404 "file not found" errors rather than a more appropriate HTTP 403 "forbidden" message; it should be noted, however, that the exact method of censorship is completely reliant on the implementing ISP; BT, for example, return 404 pages, whereas Demon return an honest message stating that, and why, the page is censored.

List of IWF filter servers on each internet provider network

By doing a traceroute to a particular website you can see the path it takes to see if it does go through the internet service providers invisible IWF filter. The following list will show the server to look for in the traceroute and be able to determine whether the website is blacklisted.

Chapter 5

Legal Status of Internet Pornography

Due to the international nature of the Internet, Internet pornography carries with it special issues with regard to the law. There is no one set of laws that apply to the distribution, purchase, or possession of Internet pornography. Only the laws of one's home nation apply with regard to distributing or possessing Internet pornography. This means that, for example, even if a pornographer is legally distributing pornography, the person receiving it may not be legally doing so due to local laws.

Areas of legal concern within many countries

Some areas of legal concern regarding adult pornography are:

- Prohibiting certain or all types of pornography that are illegal within a government's jurisdiction. For countries that do not prohibit all pornography, this might include pornography featuring violence or bestiality, for example.
- Preventing those under the legal age (for most this means a minor under 18 or 21) from accessing pornographic content.
- Enforcing laws designed to ensure that performers in pornography are of legal age.

In jurisdictions that heavily restrict access or outright ban pornography, various attempts have been made to prevent access to pornographic content. The mandating of Internet filters to try preventing access to porn sites has been used in some nations such as China and Saudi Arabia. Banning porn sites within a nation's jurisdiction does not necessarily prevent access to that site, as it may simply relocate to a hosting server within another country that does not prohibit the content it offers.

Many nations that allow at least some types of pornography attempt to ensure that those under their legal age for accessing porn (often 18 or 21) cannot easily access it. Various measures have been tried but with varying success. Within the United States, most websites have taken voluntary steps to ensure that visitors to their sites are not underage. Many Web sites provide a warning upon entry, warning minors and those not interested in viewing porn not to view the site, and requiring one to affirm that one is at least 18 and wishing to view pornographic content. Such warning pages have little effect in preventing access by minors to porn, as any minor interested in viewing the site can simply click on the "I am an adult over 18" button without having to prove his or her age.

Thus, such warnings are generally not used by themselves but with other techniques. Commercial porn sites generally do not restrict access to any pornographic content until a membership has been purchased using a credit card, as most have explicit 'free trial' content as a major part of their sales strategy. So-called age verification services have also sprung up that offer access to any Web site that participates in their program without additional charge. The users need only verify their age with the verification service, which then issues a username and password that can access all sites that use its services. Most age verification sites charge either a monthly or yearly fee to those wanting access to participating sites.

Within nations that allow at least some types of pornography, models are often required to be at least a specific age (18 is most common). Various nations have various rules as to how a site must ensure that all porn models featured on it are of age such as strict record-keeping laws.

Child pornography and the Internet

According to the United States organization The National Center for Missing and Exploited Children (NCMEC) and other international sources, child pornography is a multi-billion dollar industry and among the fastest growing criminal segments on the Internet. According to the NCMEC, approximately one fifth of all Internet pornography is child pornography.

Child pornography is illegal in most countries with coordinated enforcement by Interpol and policing institutions of various governments, including among others the United States Department of Justice. Even so, the UK based NSPCC said that worldwide an estimated 2% of websites still had not been removed a year after being identified. Recent investigations include Operation Cathedral that resulted in multi-national arrests and 7 convictions as well as uncovering 750,000 images with 1,200 unique identifiable faces being distributed over the web; Operation Amethyst which occurred in the Republic of Ireland; Operation Auxin; Operation Avalanche; Operation Ore based in the United Kingdom; Operation Pin; Operation Predator; the 2004 Ukrainian child pornography raids and the 2008 US child pornography raid. New technology that aids those who produce this material include inexpensive digital cameras and Internet distribution has made it easier than ever before to produce and distribute child pornography. The producers of child pornography try to avoid prosecution by distributing their material across national borders, though this issue is increasingly being addressed with regular arrests of suspects from a number of countries occurring over the last few years.

The legal status of simulated or "virtual" child pornography varies around the world; for example, it is legal in the United States, it is illegal in the European Union, and in Australia its legal status is unclear and so far untested in the courts. Child pornography may be simulated by the use of computers or adults made to look like children.

In 2008, it was discovered that the United States will post fake hyperlinks claiming to be child pornography and then raiding, arresting, and prosecuting anyone who was found

using the IP address that visited them, even someone whose computer was an open wifi. In 2008, a man in Middlesbrough was found guilty of downloading "child pornography" when he downloaded computer generated cartoons.

Internet pornography laws in various countries

United States

With the exception of child pornography, the legal status of accessing Internet pornography is still somewhat unsettled, though many individual states have indicated that the creation and distribution of adult films and photography are legally listed as prostitution within them.

The legality of pornography at the federal level has been traditionally determined by the Miller test, which dictates that community standards are to be used in determining whether a piece of material is obscene. Thus, if a local community determines a pornographic work to meet its standard for obscenity then it could be banned. This means that a pornographic magazine that might be legal in California could be illegal in Alabama. This standard poses a problem when it comes to the Internet because restricting the communities some pornographic material is available in is much more difficult over the Internet. It has been argued that if the Miller test were applied to the Internet then, in effect, the community standards for the most conservative community would become the standard for all U.S.-based Web sites. The courts are currently examining this issue.

The first attempt to regulate pornography on the Internet was the federal Communications Decency Act of 1996, which prohibited the "knowing" transmission of "indecent" messages to minors and the publication of materials which depict, in a manner "patently offensive as measured by contemporary community standards, sexual or excretory activities or organs", unless those materials were protected from access by minors, for example by the use of credit card systems. Immediately challenged by a group of organizations spearheaded by the ACLU, both of these provisions were struck down by the U.S. Supreme Court in Reno v. American Civil Liberties Union (1997). The "indecent transmission" and "patently offensive display" provisions were ruled to limit the freedom of speech guarantee of the First Amendment.

A second attempt was made with the narrower Child Online Protection Act (COPA) of 1998, which forced all *commercial* distributors of "material harmful to minors" to protect their sites from access by minors. "Material harmful to minors" was defined as materials that by "contemporary community standards" are judged to appeal to the "prurient interest" and that show sexual acts or nudity (including female breasts). Several states have since passed similar laws. An injunction blocking the federal government from enforcing COPA was obtained in 1998. In 1999, the 3rd Circuit Court of Appeals upheld the injunction and struck down the law, ruling that it was too broad in using "community standards" as part of the definition of harmful materials. In May 2002, the Supreme Court reviewed this ruling, found the lower court's given reason insufficient and returned the case to the circuit court. In March 2003, the 3rd Circuit Court again struck down the law

as unconstitutional, this time arguing that it would hinder protected speech among adults. The administration appealed; in June 2004 the Supreme Court upheld the injunction against the law, ruling that it was most likely unconstitutional but that a lower court should determine whether newer technical developments could have an impact on this question. On March 22, 2007, COPA was found to violate the First and Fifth Amendments of the United States Constitution and was struck down.

Another act intended to protect children from access to Internet pornography was the Children's Internet Protection Act (CIPA) of 2000. It required that public libraries, as a condition of receiving federal subsidies for Internet connectivity, employ filtering software to prevent patrons from using Internet terminals to view images of obscenity and child pornography, and to prevent children from viewing images "harmful to minors", a phrase typically used for otherwise legal pornography. The act allowed librarians to disable the filtering software for adult patrons with "bona-fide research or other lawful purposes". The act was challenged by the American Library Association on First Amendment grounds, and enforcement of the act was blocked by a lower court. In June 2003, the Supreme Court reversed and ruled that the act was constitutional and could go into effect..

The production of sexually explicit materials is regulated under 18 U.S.C. 2257, requiring "original" producers to retain records showing that all performers were over the age of 18 at the time of the production for inspection by the Attorney General. The 18 U.S.C. 2257 disclaimer is common on Internet sites distributing pornography, but the Department of Justice has rarely if ever enforced the provision. Although the law had been on the books for over 10 years, the Justice Department never actually inspected anyone. It was not until pressure from Congress, and right-wing religious groups spurred the Administration of George W. Bush and Attorney General Gonzales to begin inspections of larger commercial porn companies primarily in the Los Angeles area. Despite fearing mass inspections, harassment and prosecution, the Justice department inspected less than two dozen companies (out of several thousand operating) and no prosecutions resulted from any of the inspections. The inspections were conducted by retired FBI agents, and according to porn executives agents were always courteous and professional, and agents suggested changes or modifications to the companies record keeping process. Agents generally arrived with a list of films which they wanted to inspect the records for, most likely to avoid potential 4th amendment conflicts on issues of probable cause. Once Attorney General Alberto Gonzales departed the Justice Department, the inspections ended.

On July 1, 2005, new regulations took effect requiring among other things, "secondary" producers to retain the same records. This has been seen both as a prelude to increased inspection of records by the Department of Justice, and also as a potential assault on the Internet pornography industry by increasing the burden of compliance for distributors.

On Oct. 24, 2007 the Sixth Circuit court of appeals in Ohio, issued a judgment against the 2257 law, ruling it as unconstitutional according to the first amendment, however the Sixth Circuit subsequently reheard the case *en banc* and issued an opinion on February

20, 2009, upholding the constitutionality of the record-keeping requirements, albeit with some dissents. The Sixth Circuit en banc decision was appealed to the US Supreme Court where on Monday October 5, 2009, the US Supreme Court denied certiorari without comment not addressing the Sixth Circuit decision that 18 USC 2257 is not constitutionally "vague and overbroad" and able to be enforced.

New York sentenced ISP, BuffNET, after they plead guilty to fourth-degree criminal facilitation for not stopping child pornography after being asked to remove it.

United Kingdom

The sale or distribution of hardcore pornography through any channel was prohibited until the rules were relaxed in 2002, however the rules are still quite strict . The possession of pornographic images for private use has never been an offence in the UK. This means that UK citizens have always been able to access content on sites overseas without breaking any laws, except for child pornography.

Adult pornography that falls under the Government's classification of "extreme pornography" is illegal to possess as of January 26, 2009, carrying a three year prison sentence. This was proposed by the Government after the murder of Jane Longhurst, claiming that such material was viewed by murderer Graham Coutts. Critics of the law point out that the law will criminalise images of legal acts between consenting adults and have criticised the lack of evidence of a link between viewing such material, and violent crime. The perils behind the law are debated in the 2010 documentary Hanging Perverts.

Internet service providers started the Internet Watch Foundation in 1996 to watch for pornographic content that is in violation of British law and report it to the police. The web filter Cleanfeed is used by the largest ISP BT Group to block sites on the IWF's list which includes sites that are "criminally obscene" as well as child pornography.. The government ordered all ISPs to have a cleanfeed system by the end of 2007.

Australia

Internet pornography in Australia is subject to a multifaceted regulatory framework. Criminal legislation is in force at the Commonwealth, state and territory levels targeting those involved in the production, dissemination and consumption of illegal internet pornography (including online child abuse pornography and online pornography featuring adults portrayed as children).

It is illegal for internet content providers within Australia to 'broadcast' internet pornography classified as MA15+ to R18+ unless such internet pornography is subject to an age verification system or internet pornography which may be classified as X18+ to RC content that is not subject to an ACMA infringement notice through exceptions.

Under an internet filter, proposed by Sen. Stephen Conroy, internet pornography hosted outside Australia classified by the ACMA under the Classification Board legislation will

be blocked if such internet pornography is deemed by the AMCA to be refused classification (RC), or 'potentially' refused classification. Refused classification (RC) does include real child abuse internet pornography and bestiality internet pornography, however it may also include content discussing or illustrating examples of internet pornography (including both, illegal internet pornography and internet pornography featuring adults portrayed as children) which may limit discussion and debate to authorised statutory persons only, rather than open and free public debate.

Criminal legislation is complemented by a further tier of regulation which provides a range of administrative remedies designed to deal with the availability of inappropriate content by removing it from the internet or by blocking access to it.

Online content scheme

Since January 1999, internet pornography considered offensive or illegal has been subject to a statutory scheme administered by Australia's media regulator, the Australian Communications and Media Authority (ACMA).

Established under Schedule 5 to the *Broadcasting Services Act 1992*, the online content scheme evolved from a tradition of Australian content regulation in broadcasting and other entertainment media. This tradition embodies the principle that – while adults should be free to see, hear and read what they want – children should be protected from material that may be unsuitable for (or harmful to) them, and everyone should be protected from material that is highly offensive.

The online content scheme seeks to achieve these objectives by a number of means such as complaint investigation processes, government and industry collaboration, and community awareness and empowerment. While administration of the scheme is the responsibility of ACMA, the principle of 'co-regulation' underpinning the scheme reflects parliament's intention that government, industry and the community each plays a role in managing internet safety issues in Australia.

Investigations into internet pornography

A central feature of the online content scheme is the complaints mechanism that allows members of the Australian public to submit complaints to ACMA about offensive and illegal internet content.

Offensive and illegal internet content will be 'prohibited' under the scheme if it meets certain classification thresholds, irrespective of where the content is hosted. If prohibited content is hosted in Australia, ACMA will direct the internet content host to remove the content from its service. If prohibited content is not hosted in Australia, ACMA will notify the content to the suppliers of accredited filters in accordance with the Internet Industry Association's internet content code of practice so that access to that content is blocked for users of those filters.

In addition, sufficiently serious internet content (for example, illegal material such as child pornography) will be referred by ACMA under specialized agreements to the appropriate law enforcement agency, or, where appropriate, to a fellow member of the Internet Hotline Providers' Association (INHOPE).

Between January 2000 and June 2006, ACMA received over 5,000 complaints from the public about offensive and illegal internet content hosted in Australia and overseas, resulting in the removal or blocking of almost 4,000 individual items of online content. Approximately 60% of such content was also referred to law enforcement agencies on the basis that it related to material classifiable as 'RC' (see below).

Classification of internet pornography

Internet pornography will be 'prohibited' by ACMA if certain classification thresholds are met. These thresholds form part of the National Classification Scheme (which also applies to other forms of media such as publications, films and video games) and are agreed by the Attorneys-General of the Commonwealth, States and Territories.

The thresholds are articulated in a National Classification Code and in Guidelines. The Classification Board (part of the Attorney-General's Department) is Australia's official classification body. In the course of investigating potentially prohibited internet content, ACMA may seek a formal classification decision from the Classification Board, or it may make its own assessment of the content against the National Classification Code and in Guidelines.

In summary, the following categories of internet content are prohibited: • Content classifiable as 'RC' ('refused classification'). Such content includes, for example, illegal material (such as child sexual abuse material) and other highly offensive material (such as bestiality). • Content classifiable as 'X18+'. Such content includes material containing real depictions of actual sexual activity. • Content hosted in Australia which is classified 'R18+' and not subject to a restricted access system which complies with criteria determined by ACMA. Content classified R18+ is not considered suitable for minors. Such content includes, for example, material containing implied (or simulated) sexual activity.

Internet pornography will be prohibited if it falls within the 'RC' or 'X18+' classifications or, for content hosted in Australia that is not restricted by an adult verification procedure, if it falls within the 'R18+' classification.

Indonesia

The legal situation in Indonesia tightened sharply in 2008 with the passing of the Bill against Pornography and Pornoaction. Law books of Indonesia KUHP (Kitab Undang-Undang Hukum Perdata) article number 282 says that "it is forbidden to spread pornographic content". But there have been Indonesian pornographic pay sites with Indonesian nude models that exploit legal loopholes.

Hong Kong

Pursuant to the Control of Obscene and Indecent Articles Ordinance (Cap 390), it is an offence to publish an obscene article. Publication covers distribution, circulation, selling, hiring, giving, or lending the obscene article. Distribution by email would fall within the definition of distribution, as would the placing of an obscene article on a web site. It should also be noted that distribution does not require any element of financial gain to be present. The definition of article includes "anything consisting of or containing material to be read or looked at or both read and looked at, any sound recording, and any film, video-tape, disc or other record of a picture or pictures." The article will be considered obscene if, by reason by its obscenity, "it is not suitable to be published by any person." Obscenity includes "violence, depravity and repulsiveness". The penalty for this offence is up to three years imprisonment and a fine of up to HK$1,000,000.

Related cases:

- On January 27, 2008, The Hong Kong Police Force arrested suspects who were accused of uploading pornographic images after a multi-billion entertainment company filed a complaint about these photos available on the internet having been fabricated and might charge the offender for defamation.

Moreover, the Prevention of Child Pornography Ordinance, Cap.579, was enacted to deal with the problems associated with child pornography in Hong Kong. Under Section 3, dealing in any of the following manners with child pornography, such as “prints, makes, produces, reproduces, copies, imports or exports”; “publishes” or “has in his possession” is an offence. A child is a person under the age of 16. “Child pornography” means a photograph, film, computer-generated image or other visual depiction that is a pornographic depiction of a child. “Pornographic depiction” means a visual depiction that depicts a person as being engaged in explicit sexual conduct, whether or not the person is in fact engaged in such conduct; or a visual depiction that depicts, in a sexual manner or context, the genitals or anal region of a person or the breast of a female person.

Singapore

The Media Development Authority, a government-run agency in Singapore, blocks a "symbolic" number of websites containing "mass impact objectionable" material, including Playboy, YouPorn, and Sex.com. In addition, the Ministry of Education, Singapore blocks access to pornographic websites.

Chapter 6

Internet Assigned Numbers Authority

The **Internet Assigned Numbers Authority** (**IANA**) is the entity that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and numbers. IANA is operated by the Internet Corporation for Assigned Names and Numbers, also known as ICANN.

Prior to the establishment of ICANN for this purpose, IANA was administered primarily by Jon Postel at the Information Sciences Institute of the University of Southern California, under a contract USC/ISI had with the United States Department of Defense, until ICANN was created to assume the responsibility under a United States Department of Commerce contract.

Responsibilities

IANA is broadly responsible for the allocation of globally-unique names and numbers that are used in Internet protocols that are published as RFC documents. These documents describe methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. IANA also maintains a close liaison with the Internet Engineering Task Force (IETF) and RFC Editorial team in fulfilling this function.

In the case of the two major Internet namespaces, namely IP addresses and domain names, extra administrative policy and delegation to subordinate administrations is required because of the multi-layered distributed use of these resources.

IP addresses

IANA delegates allocations of IP address blocks to regional Internet registries (RIRs). Each RIR allocates addresses for a different area of the world. Collectively the RIRs have created the Number Resource Organization formed as a body to represent their collective interests and ensure that policy statements are coordinated globally.

The RIRs divide their allocated address pools into smaller blocks and delegate them in their respective operating regions to Internet service providers and other organizations. Since the introduction of the CIDR system, IANA typically allocates address space in the size of /8 prefix blocks for IPv4 and /12 prefix blocks from the 2000::/3 IPv6 block to requesting regional registries as needed.

Domain names

IANA administers the data in the root nameservers, which form the top of the hierarchical DNS tree. This task involves liaising with top-level domain operators, the root nameserver operators, and ICANN's policy making apparatus.

ICANN also operates the .int registry for international treaty organizations, the .arpa zone for Internet infrastructure purposes, including reverse DNS service, and other critical zones such as root-servers.org.

Protocol parameters

IANA administers many parameters of IETF protocols. Examples include the names of Uniform Resource Identifier (URI) schemes and character encodings recommended for use on the Internet. This task is undertaken under the oversight of the Internet Architecture Board, and the agreement governing the work is published in RFC 2860.

Oversight

IANA is managed by the Internet Corporation for Assigned Names and Numbers (ICANN) under contract to the United States Department of Commerce (DOC). The Department of Commerce also provides an ongoing oversight function, whereby it verifies additions and changes made in the root to ensure IANA complies with its policies.

On January 28, 2003 the Department of Commerce, via the Acquisition and Grants Office of the National Oceanic and Atmospheric Administration, issued a notice of intent to grant ICANN the IANA contract for three more years. It invited alternative offerors to submit in writing a detailed response on how they could meet the requirements themselves. Such responses were to be received no later than 10 days following publication of the invitation and the decision on whether to open the "tender" to competition was to remain solely within the discretion of the government.

In August 2006, the U.S. Department of Commerce extended its IANA contract with ICANN by an additional five years, subject to annual renewals.

Since ICANN is managing a worldwide resource, but being controlled by U.S. interests, a number of proposals have been brought forward to decouple the IANA function from ICANN. However, some believe that it would be impractical to change the current control structure without risking fracturing the Internet.

History

IANA was established informally as a reference to various technical functions for the ARPANET, that the Information Sciences Institute performed for the Defense Advanced Research Project Agency (DARPA) of the United States Department of Defense.

On March 26, 1972, Vint Cerf and Jon Postel called for establishing a socket number catalog in RFC 322. Network administrators were asked to submit a note or place a phone call, "*describing the function and socket numbers of network service programs at each HOST*". This catalog was subsequently published as RFC 433 in December 1972. In it Postel first proposed official assignments of port numbers to network services and suggested a dedicated administrative function, which he called a *czar*, to maintain a registry.

The first reference to the name "IANA" in the RFC series is in RFC 1060, published in 1990, but the function, and the term, was well established long before that; RFC 1174 says that "Throughout its entire history, the Internet system has employed a central Internet Assigned Numbers Authority (IANA)...", and RFC 1060 lists a long series of earlier editions of itself, starting with RFC 349.

In 1996 the "DNS Wars" began as the FNAC ordered the NSF to instruct its contractor, Network Solutions who ran the Internic project, to begin charging for com/net/org domain names. There was widespread dissatisfaction with this concentration of power (and money) in one company and people looked to IANA for a solution. Postel wrote up a draft on the creation of new top level domains.

USC/ISI would not back Postel in the legal sense and IANA, which was a part time "task" had no legal personality - it could not sign contracts - and there was some resentment in the community at paying IANA large sums of money to add one or two lines to the legacy root zone. Jon was trying to institutionalize IANA.

Postel was threatened by Ira Magaziner with the statement "You'll never work on the Internet again" after he split the root zone, assuming authority for the entire domain name system in an attempt to repatriate the root to IANA; Jon had plans to add hundreds of new tlds, a plan he had advocated for a while. This would let him do it, however it lasted less than a day.

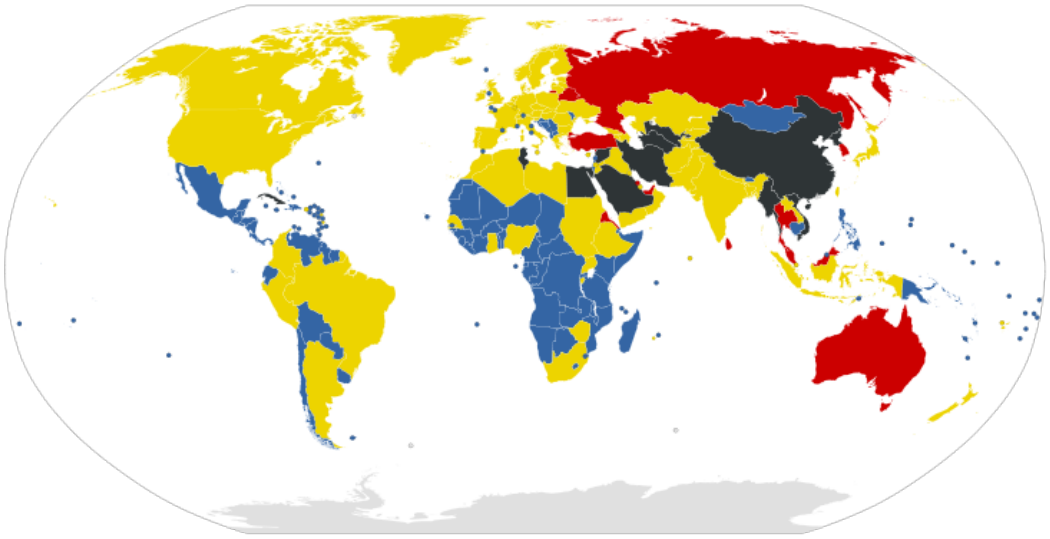
Jon Postel managed the IANA function from its inception until his death in October 1998. Postel had been given defacto authority to perform the IANA function, as he had always done it in his position at the Information Sciences Institute, under its Department of Defense contract. After his death, Joyce Reynolds, who had worked with him at IANA for many years, managed the transition of the IANA function to ICANN.

Starting in 1988, IANA was funded by the U.S. government under a contract between the Defense Advanced Research Projects Agency and Information Sciences Institute (ISI). This contract expired in April 1997, but was extended to preserve IANA's function.

- On December 24, 1998, USC entered into a transition agreement with the Internet Corporation for Assigned Names and Numbers ICANN, transferring the IANA function to ICANN, effective January 1, 1999, thus making IANA an operating unit of ICANN.
- On February 8, 2000, the Department of Commerce entered into an agreement with ICANN to perform the IANA functions.
- In June 1999, at its Oslo meeting, IETF signed an agreement with ICANN concerning the tasks that IANA would perform for the IETF; this is published as RFC 2860.
- In November 2003, Doug Barton was appointed IANA manager.
- In 2005, David Conrad was appointed as IANA manager.
- in 2010, Elise Gerich was appointed as IANA manager.

Chapter 7

Introduction to Internet Censorship



Reporters Without Borders Internet censorship ratings.
No censorship
Some censorship
Country under surveillance from Reporters Without Borders
Most heavily censored nations

Internet censorship is control or suppression of the publishing or accessing of information on the Internet. The legal issues are similar to offline censorship.

One difference is that national borders are more permeable online: residents of a country that bans certain information can find it on websites hosted outside the country. A government can try to prevent its citizens from viewing these even if it has no control over the websites themselves. Filtering can be based on a blacklist or be dynamic. In the case of a blacklist, that list is usually not published. The list may be produced manually or automatically.

Barring total control over Internet-connected computers, such as in North Korea, total censorship of information on the Internet is very difficult (or impossible) to achieve due

to the underlying distributed technology of the Internet. Pseudonymity and data havens (such as Freenet) allow unconditional free speech, as the technology guarantees that material cannot be removed and the author of any information is impossible to link to a physical identity or organization.

In some cases, Internet censorship may involve deceit. In such cases the censoring authority may block content while leading the public to believe that censorship has not been applied. This may be done by having the ISP provide a fake "Not Found" error message upon the request of an Internet page that is actually found but blocked.

In November 2007, "Father of the Internet" Vint Cerf stated that he sees Government-led control of the Internet failing due to private ownership. Many internet experts use the term "splinternet" to describe some of the effects of national firewalls.

Software

Jo Glanville, editor of Index on Censorship observes that "censorship, for the first time in its history, is now a commercial enterprise".

Technical censorship

Some commonly used methods for censoring content are:

- IP blocking. Access to a certain IP address is denied. If the target Web site is hosted in a shared hosting server, all websites on the same server will be blocked. This affects IP-based protocols such as HTTP, FTP and POP. A typical circumvention method is to find proxies that have access to the target websites, but proxies may be jammed or blocked, and some Web sites. Some large websites like Google have allocated additional IP addresses to circumvent the block, but later the block was extended to cover the new IPs.
- DNS filtering and redirection. Don't resolve domain names, or return incorrect IP addresses. This affects all IP-based protocols such as HTTP, FTP and POP. A typical circumvention method is to find a domain name server that resolves domain names correctly, but domain name servers are subject to blockage as well, especially IP blocking. Another workaround is to bypass DNS if the IP address is obtainable from other sources and is not blocked. Examples are modifying the Hosts file or typing the IP address instead of the domain name in a Web browser.
- Uniform Resource Locator (URL) filtering. Scan the requested URL string for target keywords regardless of the domain name specified in the URL. This affects the HTTP protocol. Typical circumvention methods are to use escaped characters in the URL, or to use encrypted protocols such as VPN and TLS/SSL.
- Packet filtering. Terminate TCP packet transmissions when a certain number of controversial keywords are detected. This affects all TCP-based protocols such as HTTP, FTP and POP, but Search engine results pages are more likely to be censored. Typical circumvention methods are to use encrypted connections - such

as VPN and TLS/SSL - to escape the HTML content, or by reducing the TCP/IP stack's MTU/MSS to reduce the amount of text contained in a given packet.
- Connection reset. If a previous TCP connection is blocked by the filter, future connection attempts from both sides will also be blocked for up to 30 minutes. Depending on the location of the block, other users or websites may also be blocked if the communication is routed to the location of the block. A circumvention method is to ignore the reset packet sent by the firewall.
- Reverse surveillance. Computers accessing certain websites including Google are automatically exposed to reverse scanning from the ISP in an apparent attempt to extract further information from the "offending" system.

One of the most popular filtering software programmes is SmartFilter, owned by Secure Computing in California, which has recently been bought by McAfee. SmartFilter has been used by Tunisia, Saudi Arabia and Sudan, as well as in the US and the UK.

"By-catch"

Automatic censorship sometimes stops matter which it was not intended to stop. An example is that automatic censorship against sexual words in matter for children, set to block the word "cunt", has been known to block the Lincolnshire (UK) placename Scunthorpe.

Circumvention

There are a number of resources that allow users to bypass the technical aspects of Internet censorship. Each solution has differing ease of use, speed, and security from other options. Most, however, rely on gaining access to an internet connection that is not subject to filtering, often in a different jurisdiction not subject to the same censorship laws. This is an inherent problem in internet censorship in that so long as there is one publicly accessible system in the world without censorship, it will still be possible to have access to censored material.

Java Anon Proxy

Java Anon Proxy is primarily a strong, free and open source anonymizer software available for all operating systems. As of 2004, it also includes a blocking resistance functionality that allows users to circumvent the blocking of the underlying anonymity service AN.ON by accessing it via other users of the software (forwarding client).

The addresses of JAP users that provide a forwarding server can be retrieved by getting contact to AN.ON's InfoService network, either automatically or, if this network is blocked, too, by writing an e-mail to one of these InfoServices. The JAP software automatically decrypts the answer after the user completes a CAPTCHA. The developers are currently planning to integrate additional and even stronger blocking resistance functions.

Virtual Private Networks (VPNs)

Using Virtual Private Networks, a user who experiences internet censorship can create a secure connection to a more permissive country, and browse the internet as if they were situated in that country. Some services are offered for a monthly fee, others are ad-supported.

I2P

I2P is open source software that can be used for anonymous surfing, chatting, blogging and file transfers, among other things.

JonDos

JonDos is based on open source software and provides secure and fast anonymizing networking.

Sneakernets

Sneakernet is a term used to describe the transfer of electronic information, especially computer files, by physically carrying data on storage media from one place to another. A sneakernet can move data regardless of network restrictions simply by not using the network at all.

Around the world

The following sections follow the OpenNet Initiative (ONI) categorization scheme: Pervasive, Substantial, Nominal, Indirect, Watchlist.

In 2006, Reporters without Borders (*Reporters sans frontières*, RSF, a Paris-based international non-governmental organization that advocates freedom of the press) published a list of the 13 "enemies of the Internet": The organization classifies a country as an enemy of the internet because "all of these countries mark themselves out not just for their capacity to censor news and information online but also for their almost systematic repression of Internet users." The list is updated annually and now includes 12 countries in 2009:

-  Burma
-  China
-  Cuba
-  Egypt
-  Iran
-  North Korea
-  Saudi Arabia
-  Syria
-  Tunisia

- Turkmenistan
- Uzbekistan
- Vietnam

On the 12th, March 2010, Reporters Without Borders published the updated list of the Internet Enemies.

Pervasive

While there is no universally agreed upon definition of what constitutes "pervasive censorship", RSF (*Reporters sans frontières*) maintains an internet enemy list while the OpenNet Initiative categorizes some nations as practicing extreme levels of Internet censorship. Such nations often censor political content and may retaliate against citizens who violate the censorship with imprisonment or other sanctions.

Afghanistan

The Electronic Frontier Foundation reported that the Afghan Ministry of Communications mandated in June 2010 that all Internet Service Providers (ISPs) in Afghanistan filter Facebook, Gmail, Twitter, YouTube and websites related to alcohol, gambling and sex. They are also trying or blocking websites which are “immoral” and against the traditions of the Afghan people. However, executives at Afghan ISPs said this was the result of a mistaken announcement by Ariana Network Service, one of the country's largest ISPs. An executive there said that while the government intends to censor pornographic content and gambling sites, social networking sites and email services are not slated for filtering. As of July 2010, enforcement of Afghanistan's restrictions on "immoral" content was limited, with internet executives saying the government didn't have the technical capacity to filter internet traffic.

Egypt

Egypt is not categorized by the ONI and is on the RSF's internet enemy list. Due to fears of terrorism, the government increased web surveillance in 2007. To connect to wireless internet in a public place, such as a cybercafé, a person must give up a lot of personal information, such as a phone number or ID #, making it hard for citizens to express themselves freely.

Syria

Syria has banned websites for political reasons and arrested people accessing them, and is in ONI's pervasive category and is on RSF's internet enemy list. In addition to filtering a wide range of Web content, the Syrian government monitors Internet use very closely and has detained citizens "for expressing their opinions or reporting information online." Vague and broadly worded laws invite government abuse and have prompted Internet users to engage in self-censoring and self-monitoring to avoid the state's ambiguous grounds for arrest.

Turkmenistan

Turkmenistan is not categorized by the ONI and it is on the RSF's internet enemy list. Internet usage in Turkmenistan is under tight control by the government. Turkmen got their news through satellite television until 2008 when the government decided to get rid of satellites leaving Internet as the only medium where information could be gathered. Internet is monitored thoroughly by the government as websites ran by human rights organizations and news agencies were blocked. Attempts to get around this censorship could lead to grave consequences

Uzbekistan

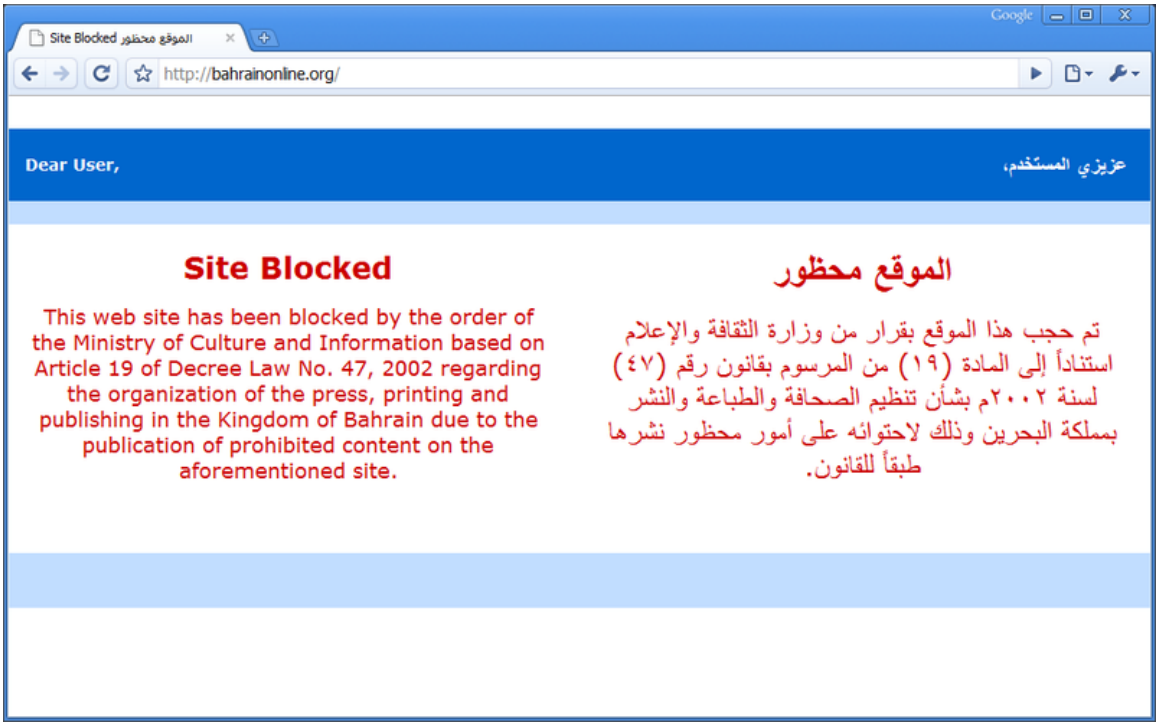
Uzbekistan is in ONI's pervasive category and is on RSF's internet enemy list. Uzbekistan prevents access to websites regarding banned Islamic movements, independent media, NGOs, and material critical of the government's human rights violations. Some Internet cafes in the capital have posted warnings that users will be fined for viewing pornographic websites or website containing banned political material. The main VoIP protocols SIP and IAX used to be blocked for individual users; however, as of July 2010, blocks were no longer in place. Facebook was blocked for few days in 2010.

Venezuela

On December 2010 the government of Venezuela led by Hugo Chavez passed a law for the regulation of contents in the Internet. The National Assembly which is controlled by a pro Chavez majority approved a law named Social responsibility in Radio, Television and Electronic Media (*Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos*) The law is intended to exercise control over content that could "entice felonies", "create social distress" and the ones dedicated to "question the legitimate constituted authority". The law indicates that website's owners will be responsible for the information and contents published and that they will have to create mechanisms that could restrict without delay the distribution of content that could go against the aforementioned restrictions. The fines to those individuals that break the law will be of the 10% of the person's last year's income. The law was received with criticism from the opposition on the grounds that it is considered a violation to the protection to the freedom of speech as stipulated in the Venezuelan constitution and a reform that encourages censorship and self-censorship.

Substantial

Bahrain



A Bahraini website blocked

On 5 January 2009 the Ministry of Culture and Information issued an order (Resolution No 1 of 2009) pursuant to the Telecommunications Law and Press and Publications Law of Bahrain that regulates the blocking and unblocking of websites. This resolution requires all ISPs - among other things - to procure and install a website blocking software solution chosen by the Ministry. The Telecommunications Regulatory Authority ("TRA") assisted the Ministry of Culture and Information in the execution of the said Resolution by coordinating the procurement of the unified website blocking software solution. This software solution is operated solely by the Ministry of Information and Culture and neither the TRA nor ISPs have any control over sites that are blocked or unblocked.

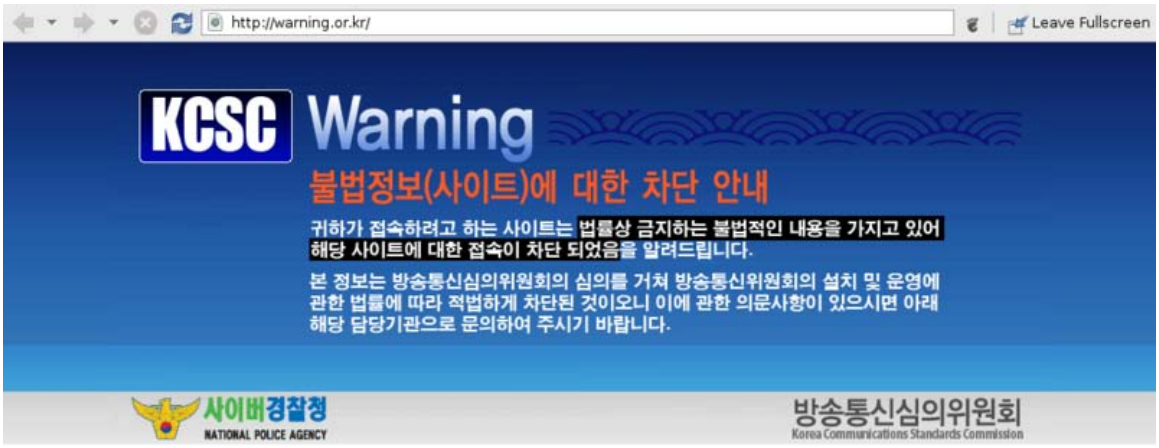
Oman

Many websites and services, including Youtube, Vtunnel, Ktunnel, Skype and other sites, are blocked due to their being "against the culture of Sultanate of Oman". It is impossible to overcome the censor by using a program to mask IP and DNS.

South Korea

South Korea is in ONI's substantial category and also listed on an "Enemy of the Internet" by Reporters Without Borders (RSF) for its "draconian" censorship. South

Korea's internet censorship policy is highly political and particularly strong toward suppressing anonymity in the Korean internet. In 2007, numerous bloggers were censored and their posts deleted by police for expressing criticism of, or even support for, presidential candidates. This even lead to some bloggers being arrested by the police. Subsequently in 2008, just before a new presidential election, new legislation that required all major internet portal sites to require identity verification of their users was put into effect. This applies to all users who add any publicly viewable content. For example, to post a comment on a news article, a user registration and citizen identity number verification is required. For foreigners who do not have such numbers, a copy of passport must be faxed and verified. Although this law was initially met with public outcry, as of 2008, most of the major portals, including Daum, Naver, Nate, and Yahoo Korea, enforce such verification before the user can post any material that is publicly viewable.



사이트분야	담당기관	전화번호
안보위해행위	경 찰 청	1566 - 0112
도 박	경 찰 청	1566 - 0112
음 란	방송통신심의위원회 통신심의실	(02)3219 - 5286, 5155
불법 건강식품 판매, 식품과대 광고	식품의약품안전청 식품관리과	(02)380 - 1633
불법 의약품 및 화장품 판매	식품의약품안전청 의약품관리과	(02)3156 - 8061
불법 마약류 제조 및 판매	식품의약품안전청 마약오남용의약품과	(02)3156 - 8085
불법 경주권 구매대행	국민체육진흥공단 경륜운영본부	(02)2067 - 5813

Illegal content blocked

Also, South Korea has banned at least 31 sites considered sympathetic to North Korea through the use of IP blocking. Moreover, they started to block illegal websites such as unrated games, pornography, gambling, etc., since 2008. Attempts to access these sites are automatically redirected to the warning page showing "This site is legally blocked by the government regulations."

Furthermore, search engines are required to verify age for some keywords deemed inappropriate for minors. For such keywords, age verification using national identity number is required. For foreigners, a copy of passport must be faxed to verify the age. As of 2008, practically all large search engine companies in South Korea, including foreign-owned companies (e.g. Yahoo! Korea), have complied with this legislation. Only Google evades government's legislation. In April 2009 when Communication Commission ordered to put on user verification system at YouTube, Google Korea blocked video uploading from users whose country setting is Korean.

Saudi Arabia

Saudi Arabia is in ONI's substantial category and is on RSF's internet enemy list. Saudi Arabia directs all international Internet traffic through a proxy farm located in King Abdulaziz City for Science & Technology. Content filtering is implemented there using software by Secure Computing. Additionally, a number of sites are blocked according to two lists maintained by the Internet Services Unit (ISU): one containing "immoral" (mostly pornographic) sites, the other based on directions from a security committee run by the Ministry of Interior (including sites critical of the Saudi government). Citizens are encouraged to actively report "immoral" sites for blocking, using a provided Web form. The legal basis for content-filtering is the resolution by Council of Ministers dated 12 February 2001. According to a study carried out in 2004 by the OpenNet Initiative:

The most aggressive censorship focused on pornography, drug use, gambling, religious conversion of Muslims, and filtering circumvention tools.

United Arab Emirates

The United Arab Emirates is in ONI's substantial category and is not on Reporters Without Borders (RSF)'s internet enemy list. The United Arab Emirates forcibly censors the Internet using Secure Computing's solution. The nation's ISPs Etisalat and du (telco) ban pornography, politically sensitive material, all Israeli domains, and anything against the perceived moral values of the UAE. All or most VoIP services are blocked.

Sri Lanka

Sri Lanka is in the RSF's list of Countries under surveillance. Currently several political and news websites, including tamilnet.com and lankanewsweb.com has been blocked in country.

Also Sri Lanka court recently ordered to block more than 300 adult sites to "protect women and children"

Yemen

Yemen is in ONI's substantial category and is not on RSF's internet enemy list. Yemen's two ISPs block access to contents falling under the categories of gambling, adult

contents, and sex education as well as material seeking to convert Muslims to other religions.

Nominal and others

Belarus

Belarus is in ONI's watchlist and was for some time on RSF's internet enemy list. OpenNet Initiative suspect internet filtering on political and social issues.

Belgium

Belgian internet providers Belgacom, Telenet, Base, Scarlet, EDPnet, Dommel, Proximus, Mobistar, Mobile Vikings, Tele2, and Versatel have started filtering several websites on DNS level since April 2009. People who browse the internet using one of these providers and hit a blocked website are redirected to a page that claims that the content of the website is illegal under Belgian law and therefore blocked.

Brazil

Brazilian legislation restricts the freedom of expression (Paim Law), directed especially to publications considered racist (such as neo-nazi sites). The Brazilian Constitution also prohibits anonymity of journalists.

Canada

Canada is in ONI's nominal category and is not on RSF's internet enemy list. In a few cases, information which the government is actively attempting to keep out of Canadian broadcast and print media (such as names of young offenders or information on criminal trials subject to publication bans) is available to Canadian users via Internet from sites hosted outside Canada.

Project Cleanfeed Canada (cybertip.ca) decides what sites are child pornographic in nature and transmits those lists to the voluntarily participating ISPs who can then block the pages for their users. However, some authors, bloggers and digital rights lawyers argue that they are accountable to no one and could be adding non pornographic sites to their list without public knowledge.

Chile

Chile is not categorized by ONI and is not on RSF's internet enemy list. Many educational institutions (universities and schools) block the access to websites like YouTube, Fotolog, Flickr, Blogger, Rapidshare, Twitter and Facebook, depending of the institution; in some cases also popular portals like Terra.cl, LUN.com, EMOL.com are also blocked; pornography, especially any kind of child pornographic website is blocked. The Chilean Government also block the access in their computers to blogs or electronic

versions of the local newspapers with opinions against the Government or the ruling coalition, for example, during the first days of Transantiago or the 2006 Student Protests.

Colombia

Colombia blocks several websites as part of its Internet Sano program.In December 2009, an internaute was sent to prison for threatening president Álvaro Uribe's sons.

Czech Republic

Since 2008, mobile operators T-Mobile and Vodafone pass mobile and fixed Internet traffic through Cleanfeed, which uses data provided by the Internet Watch Foundation to identify pages believed to contain indecent photographs of children, and racist materials.

On August 13, 2009, Telefónica O2 Czech Republic, Czech DSL incumbent and mobile operator, started to block access to sites listed by Internet Watch Foundation. The company said it wanted to replace the list with data provided by Czech Police. The rollout of the blocking system attracted public attention due to serious network service difficulties and many innocent sites mistakenly blocked. The concrete blocking implementation is unknown but it is believed that recursive DNS servers provided by the operator to its customers have been modified to return fake answers diverting consequent TCP connections to an HTTP firewall.

On May 6, 2010, T-Mobile Czech Republic officially announced that it was starting to block web pages promoting child pornography, child prostitution, child trafficking, pedophilia and illegal sexual contact with children. T-Mobile claimed that its blocking was based on URLs from the Internet Watch Foundation list and on individual direct requests made by customers.

Denmark

Denmark is not categorized by ONI and is not on RSF's internet enemy list. Denmark's biggest Internet service provider TDC A/S launched a DNS-based child pornography filter on 18 October 2005 in cooperation with the state police department and Save the Children, a charity organisation. Since then, all major providers have joined and as of May 2006, 98% of the Danish Internet users are restricted by the filter. The filter caused some controversy in March 2006, when a legal sex site named Bizar.dk was caught in the filter, sparking discussion about the reliability, accuracy and credibility of the filter. Also, as of 18 October 2005, TDC A/S has blocked access to AllOfMP3.com, a popular MP3 download site, through DNS filtering.

4 February 2008 a Danish court has ordered the Danish ISP Tele2 to shutdown access to the filesharing site thepiratebay.org for all its Danish users.

On 23 December 2008, the list of 3,863 sites filtered in Denmark was released by Wikileaks.

Estonia

Early 2010 Estonia started DNS filtering of "remote gambling sites" conflicting the renewed Gambling Act (2008). Estonia Implements Gambling Act. So far (2010-03-01) only one casino has obtained the proper license. The Gambling Act says - servers for the "legal" remote gambling **must** be physically located in Estonia. The latest local news is that Tax and Customs Board has compiled a blocking list containing 175 sites which ISPs are to enforce. Previously Internet was completely free of censorship in Estonia.

Fiji

Fiji is not categorized by ONI and is not on RSF's internet enemy list. In May 2007 it was reported that the military in Fiji had blocked access to blogs critical of the regime.

Finland

Finland is not categorized by ONI and is not on RSF's internet enemy list. Following a "voluntary law" enacted by Finnish parliament in 1 January 2007, most of the Finland's major Internet service providers decided on 22 November 2006 to begin filtering child pornography and ISPs first started filtering on January 2008. The Ministry of Communications has commented that filtering is voluntary for ISPs as long as they do not refuse. The blacklist is provided by Finnish police and should contain only foreign sites. Technically filtering was planned to be URI based like the United Kingdom's Cleanfeed, but so far implementations have been DNS based.

A majority of these censored Internet sites, however, do not actually seem to be censored by the Finnish ISPs due to actual child pornography, but due to "normal" adult pornography instead. Most of the known sites are also located in EU or United States where child pornography is strictly illegal anyway. Two-thirds of the Finnish internet censorship list of the filtered domains were collected on lapsiporno.info, the homepage of Matti Nikki, a Finnish activist criticizing Internet censorship in the European Union and especially in Finland. On 12 February 2008, Nikki's page was also added to National Bureau of Investigation's blacklist. As the list was compiled using links from pornography sites, this list does not tell anything about the last third of the blocked sites.

At September 2008 problems with accuracy continued, when websites of main international standards organization for World Wide Web W3C was briefly blacklisted as childporn by mistake.

More recently, a government-sponsored report has considered establishing similar filtering in order to curb online gambling.

After investigation of complaints about how the law on filtering child pornography has been implemented and the actions of the police, the vice Parliamentary Ombudsman concluded on 29.5.2009 that the police had followed the law and that most sites on the list did have material that could be classified as child pornography at the time they were

investigated by the police. He also found that the law is somewhat unclear and that its effect on free speech is problematic and recommends these matters be considered when the law is overseen.

France

France is in ONI's watchlist and is not on RSF's internet enemy list. French courts demanded Yahoo! block Nazi material in the case LICRA vs. Yahoo. The case is currently on appeal for an en banc rehearing.

The Hadopi law, enacted in 2009, allows disconnecting from the Internet users that have been caught illegally downloading copyrighted content, or failing to secure their system again such illegal downloads; as of August 2009, this law is to be supplemented by a Hadopi2 law. The LOPPSI 2 law, brought before Parliament in 2009, will authorize a blacklist of sites providing child pornography, established by the Ministry of the Interior, which Internet service providers will have to block. The Loppsi "Bill on direction and planning for the performance of domestic security" is a far-reaching security bill that seeks to modernise Internet laws, criminalising online identity theft, allowing police to tap Internet connections as well as phone lines during investigations and targeting child pornography by ordering ISPs to filter Internet connections.

In 2010, French parliament opposed all the amendments seeking to minimise the use of filtering Internet sites. This move has stirred controversy throughout French society, as the Internet filtering intended to catch child pornographers could also be extended to censor other material.

Critics also warn that filtering URLs will have no effect, as distributors of child pornographer and other materials are already using encrypted peer-to-peer systems to deliver their wares.

Georgia

Georgia blocked all websites with addresses ending in .ru (top-level domain for Russian Federation) after South Ossetia War in 2008.

Israel

Israel is not categorized by ONI and is not on RSF's internet enemy list. The Orthodox Jewish parties in Israel proposed an internet censorship legislation would only allow access to adult-content Internet sites for users who identify themselves as adults and request not to be subject to filtering. In 27/02/2008 the law passed in its first of three votes required, however it has been rejected by the government's legislation committee on 12/07/2009.

Jordan

Jordan is not on RSF's internet enemy list and censorship is relatively light. Access to Internet content in the Hashemite Kingdom of Jordan remains largely unfettered, with filtering selectively applied to only a small number of sites. However, media laws and regulations encourage some measure of self-censorship in cyberspace, and citizens have reportedly been questioned and arrested for Web content they have authored. Censorship in Jordan is mainly focused on political issues that might be seen as a threat to national security due to the nation's close proximity to regional hotspots like Israel, Iraq, Lebanon, and the Palestinian territories. Jordan, unlike most of its neighbors, has a free and an advanced telecommunications sector.

Malaysia

There have been mixed messages and confusion regarding Internet censorship in Malaysia. Prime Ministers Abdullah Badawi and Najib Tun Razak, on many occasions, have pledged that Internet access in Malaysia will not be censored and that it is up to parents to install their own censorship software and provide education to their children (provide self-censorship). The ISPs also actively deny that there are Internet filters in place when asked. However, the Communications Minister has occasionally announced that they are working on a nationwide filter, but each time such an announcement is made the Prime Minister makes a rebuttal to emphasize that there will be no Internet censorship. The state ministries of Terengganu and Kelantan have also announced that they have statewide filters in place in their respective states.

Porn sites such as Pornhub.com and Tube8.com are blocked without any notice or reason.

In 2006 Deputy Science and Technology Minister Kong Cho Ha has announced that all Malaysian news blogs will have to be registered with the Ministry of Information. He justified this by stating the law was necessary to dissuade bloggers from promoting disorder in Malaysia's multi-ethnic society.

The web page faithfreedom.org, which expresses a critical view on Islam, is blocked in Malaysia (December 2010).

WikiLeaks, the popular whistle-blowing site, has also been blocked by the Malaysian ISPs. Trying to access countries under categories brings a 'Link is Broken' error message for the user.

Netherlands

Since 2007 in the Netherlands one major ISP, UPC Netherlands, blocks access on DNS level to sites authorities claim are known to provide child pornography. In the second quarter of 2008 all major Dutch ISPs have agreed with Ernst Hirsch Ballin of the Ministry of Justice to also block all the sites that are on the list. The blacklist is compiled by the National Police Forces (KLPD). Ernst Hirsch Ballin has said that at the moment

150 websites are blocked. It contains no websites that are hosted in EU countries and they are checked once every 2 months by Productteam Bestrijding Kinderpornografie. Providers will not be forced to use it since that would be unconstitutional according to a research done by the governmental Scientific Research- and Documentation Center (WODC) commissioned by the Ministry of Justice. As of 2009 the only providers that use the filter are UPC and two small providers, Scarlet and Kliksafe. The providers that have been positive about a non-mandatory filter do not have it in use.

Norway

Norway is in ONI's watchlist and is not on RSF's internet enemy list. Norway's major Internet service providers have a DNS filter which blocks access to sites authorities claim are known to provide child pornography, similar to Denmark's filter. A list claimed to be the Norwegian DNS blacklist was published at Wikileaks in March 2009. The minister of justice, Knut Storberget, sent a letter threatening ISPs with a law compelling them to use the filter should they refuse to do so voluntarily (dated August 29, 2008).

Poland

As of December 2008, Poland's main ISP, TPSA, started to occasionally block some websites, which they deem "improper".

At present some legalisations about Internet censorships are proposed. There are propositions to build Register of blocked web sites, based on government organ choice (Police, Ministry of Finance, Secret Police etc.). In project administrative decisions, without court intervention, may be performed, and then chosen address would be blocked. Owner of the site would not be informed until performing blockade. Then may be possible to follow procedure to legalise blocked site.

Russia

Russia is in ONI's watchlist and is not on RSF's internet enemy list. OpenNet Initiative found no evidence of internet filtering. Russia pressured Lithuania into shutting down the Kavkaz Center website, a site that supports creation of a Sharia state in North Caucasus and hosts videos on terrorist attacks on Russian forces in North Caucasus.

Singapore

Singapore is in ONI's nominal category and is not on RSF's internet enemy list. In Singapore, three people were arrested and charged with sedition for posting racist comments on the Internet, of which two have been sentenced to imprisonment. Some ISPs also block internet content related to recreational drug use. Singapore's government-run Media Development Authority maintains a confidential list of blocked websites that are inaccessible within the country. The Media Development Agency exerts control over Singapore's three ISPs to ensure that blocked content is entirely inaccessible.

Slovenia

Slovenian National Assembly on 28 January 2010 accepted new changes to the law governing gambling which legalized Internet censorship in Slovenia, although currently just for Internet gambling web sites that run without permission of the Slovenian government. The law makes Internet service providers responsible for accessing those sites and thus requires them to install censorship equipment/systems which currently they have not yet had.

Sweden

Sweden is not categorized by ONI and is not on RSF's internet enemy list. Sweden's major Internet service providers have a DNS filter which blocks access to sites authorities claim are known to provide child porn, similar to Denmark's filter. A partial sample of the Swedish internet censorship list can be seen at a Finnish site criticizing internet censorship. The Swedish police are responsible for updating this list of forbidden Internet sites. On 6 July, Swedish police said that there is material with child pornography available on torrents linked to from the torrent tracker site Pirate Bay and said it would be included in the list of forbidden Internet sites. This, however, did not happen as the police claimed the illegal material had been removed from the site. Police never specified what the illegal content was on TPB. This came with criticism and accusations that the intended The Pirate Bay's censorship was political in nature.

Others

Mexico

In May 2009, the Mexican Federal Electoral Institute (IFE), asked YouTube to remove a parody of Fidel Herrera, governor of the state of Veracruz. Negative advertising in political campaigns is prohibited by present law, although the video appears to be made by a regular citizen which would make it legal. It was the first time a Mexican institution intervened directly with the Internet.

As of 2010, Mexico does not censor websites.

Portal censorship

Major portals occasionally exclude web sites that they would ordinarily include. This renders a site invisible to people who do not know where to find it. When a major portal does this, it has a similar effect as censorship. Sometimes this exclusion is done to satisfy a legal or other requirement, other times it is purely at the discretion of the portal.

Examples

- Google.de and Google.fr remove Neo-Nazi and other listings in compliance with German and French law.

Major web portal official statements on site removal

- Google: "Google may temporarily or permanently remove sites from its index and search results if it believes it is obligated to do so by law, if the sites do not meet Google's quality guidelines, or for other reasons, such as if the sites detract from users' ability to locate relevant information."
- Yahoo!: Yahoo!'s terms of service state that they reserve the right to "pre-screen, refuse or remove" any content that they feel violates the terms of service or deem distasteful; however, removing information is never obligatory. Yahoo! also does not reserve the right to pre-screen any information.

Chapter 8

Internet Censorship in Iran

In the first few years of the 21st century, Iran experienced a great surge in Internet usage, and, with 20 million people on the Internet, currently has the second highest percentage of its population online in the Middle East, after Israel. When initially introduced, the Internet services provided by the government within Iran were comparatively open. Many users saw the Internet as an easy way to get around Iran's strict press laws. A clampdown started with the election of Iranian president Mohammad Khatami, and the start of the 2nd of Khordad reform movement. It worsened with the administration of conservative president Mahmoud Ahmadinejad in 2005. Regime opponents in Iran are said to rely heavily on Web-based communication with the outside world.

Many bloggers, online activists, and technical staff have faced jail terms, harassment and abuse. In November 2006, Iran was one of 13 countries labeled "enemies of the internet" by activist group Reporters Without Borders. In March 2010, it was one of twelve regimes so labeled. Following the 2009 Iranian presidential election, the U.S. Senate ratified a plan to help curb "censorship in the Islamic Republic". The legislation dubbed the Victims of Iranian Censorship (VOICE) Act was allocated $50 million to fund measures "to counter Iranian government efforts to jam radio, satellite, and Internet-based transmissions."

Recently, the Iran government required all Iranians to register their web sites in Ministry of art and culture. They also plan to filter all other websites up to March 2007.

Internet service providers

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. 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. The state blacklist consists of about 15,000 websites forbidden by the Iranian government. Before subscribers can access Internet service providers, they must first promise in writing not to access "non-Islamic" sites. In 2008, Iran has blocked access to more than five million Internet sites, whose content is mostly perceived as immoral and anti-social. In recent years, Internet service providers have been told to block access to political, human rights and women's sites and weblogs expressing dissent or deemed to

be pornographic and anti-Islamic. The ban has also targeted such popular social networking sites as Facebook, Twitter and YouTube, as well as news sites.

Software

The primary engine of Iran's censorship is the content-control software SmartFilter, developed by San Jose firm Secure Computing. However, Secure denies ever having sold the software to Iran, and alleges that Iran is illegally using the software without a license.

As of 2006, Iran's SmartFilter is configured to filter local Persian-language sites, and block prominent English-language sites, such as the websites for the New York Times, Amazon.com, IMDB.com and Facebook.

The software effectively blocks access to most pornographic sites, gay and lesbian sites, reformist political sites, news media, sites that provide tools to help users cloak their Internet identity, and other sites nebulously defined as immoral on various grounds. Iran has been accused by its critics of censoring more Internet sites than any other nation except China.

Iran has since developed its own hardware and software for filtering purposes. The architecture of the Iranian Internet is particularly conducive to widespread surveillance as all traffic from the dozens of ISPs serving households is routed through the state-controlled telecommunications infrastructure of the Telecommunication Company of Iran (TCI).

American proxy server

Iranians can sometimes access forbidden sites through proxy servers, although these machines can be blocked as well. In 2003, the United States began providing a free proxy server to Iranian citizens through its IBB service Voice of America with Internet privacy company Anonymizer, Inc. The proxy website changes whenever the Iranian government blocks it.

However, even the U.S. proxy filters pornographic websites and keywords. "There's a limit to what taxpayers should pay for," an IBB program manager was quoted as saying. The forbidden keywords are controversial—banning "gay" effectively bars access to a host of gay and lesbian sites—and have had unintended consequences. The banning of "ass", for example, blocks access to the website of the United States Embassy. A complete list of the blacklisted keywords on the American server can be found here.

Deep packet inspection

The possibility that Nokia Siemens Systems sold, in 2008, TCI a deep packet inspection countrywide capacity for monitoring or even altering content of Internet voice and mail communication was raised in a *Wall Street Journal* report in June, 2009. The company

has denied that what it sold to TCI had such capacity but only "lawful intercept" capacity relative to child pornography e.g.

Internet connection speed restrictions

In October 2006, the Iranian government ordered all ISPs to limit their download speeds to 128kbit/s for all residential clients and internet cafes. Although no reason for the decree was given, it is widely believed the move was designed to reduce the amount of western media (e.g. films and music) entering the country. There is also a newfound state awareness of how domestically produced content considered undesirable can pervade the internet, highlighted by the 2006 controversy over the appearance of a celebrity sex tape featuring a popular Iranian soap opera actress (or a convincing look-alike).

As of 2010, most major ISPs in Tehran offer 1Mbit/s for 2,190,000 Rials/Month (around 220 Dollars/Month), 2Mbit/s for 3,950,000 Rials/Month (around 400 Dollars/Month) for unlimited data traffic. 1Mbit/s with 2GB traffic limitation costs 18,900 Rials/Month (around 19 Dollars/Month). Note that restriction for residential clients speed of 128Kb/s is still in place and the speeds mentioned above is just for offices and commercial firms.

Note that you have to pay this every month and for a year the price is multiplied by 12 that makes a 1Mbit/s subscription 26,280,000 Rials/Year (around 2,600 Dollars/Year).

The Internet price is even higher in other cities, as the infrastructure is either doesn't exist or is way too old. Not to mention that the government is doing nothing to reduce the prices, and the Internet speed and price issues are boycotted by the national TV and radio channels.

Monitoring

According to the American newspaper Washington Times, Iran is using an electronic surveillance system to monitor communications by political dissidents on the internet. A monitoring center installed by Nokia Siemens Networks (NSN) for Irantelecom intercepts Web-based communications and archives them for the Iranian government. Lily Mazahery, a human rights and immigration lawyer who represents Iranian dissidents, reported that one of her clients was arrested because of instant messaging he had participated in with Ms. Mazahery,

"He told me he had received a call from the Ministry of Intelligence, and this guy when he went to the interrogation, they put in front of him printed copies of his chats with me. He said he was dumbfounded, and he was sent to prison."

Andrew Lighten, a NSN employee, however, states that the company has not provided Deep Packet Inspection software for the Internet to Iran, but only monitoring and deep packet inspection software for 3G UMTS mobile networks, which he states, actually require this kind of technique to be present wherever they are implemented.

According to a newly passed legislation, Internet Service Providers (ISP) in Iran are required to store all the data sent or received by each of their clients. ISPs may delete the data no sooner than 3 months after the expiry of each client's contract.

Out of country protests following the 2009 elections resulted in Iran increasing their monitoring of online social networks, especially targeting Facebook. Upon re-entry to the country, citizens that have lived abroad have been questioned and detained due to the contents of their personal Facebook pages.

Chapter 9

Internet Censorship in the People's Republic of China

Internet censorship in the People's Republic of China is conducted under a wide variety of laws and administrative regulations. There are no specific laws or regulations which the censorship follows. In accordance with these laws, more than sixty Internet regulations have been made by the People's Republic of China (PRC) government, and censorship systems are vigorously implemented by provincial branches of state-owned ISPs, business companies, and organizations.

The censorship is not applied in Hong Kong and Macau, as they are special entities recognized by international treaty vested with independent judicial power and not subject to most laws of the PRC, including those requiring the restriction of free flow of information.

The escalation of the government's effort to neutralize critical online opinion comes after a series of large anti-Japanese, anti-pollution, anti-corruption protests, and ethnic riots, many of which were organized or publicized using instant messaging services, chat rooms, and text messages. The size of the Internet police is rumored at more than 50,000. Critical comments appearing on Internet forums, blogs, and major portals such as Sohu and Sina usually are erased within minutes.

The apparatus of the PRC's Internet repression is considered more extensive and more advanced than in any other country in the world. The regime not only blocks website content but also monitors the Internet access of individuals. Amnesty International notes that China “has the largest recorded number of imprisoned journalists and cyber-dissidents in the world.” The offences of which they are accused include communicating with groups abroad, opposing the persecution of the Falun Gong, signing online petitions, and calling for reform and an end to corruption.

Beginning of Regulations

China started its Internet censorship with three regulations issued by China’s central government. The first regulation was called the Temporary Regulation for the Management of Computer Information Network International Connection. The regulation

was passed in the 42nd Standing Convention of the State Council on January 23, 1996. It was formally announced on February 1, 1996, and updated again on May 20, 1997.

The content of the first regulation states, “ No units or individuals are allowed to establish direct international connection by themselves.” (Item 6) “All direct linkage with the Internet must go through ChinaNet, GBNet, CERNET or CSTNET. A license is required for anyone to provide Internet access to users.” (Item 8) The second regulation was the Ordinance for Security Protection of Computer Information Systems. It was issued on February 18, 1994 by the State Council to give the responsibility of Internet security protection to the Ministry of Public Security, which is entitled to “supervise, inspect and guide the security protection work”, and to “investigate and prosecute illegal criminal cases” (Item 17)

The Ordinance regulation further led to the Security Management Procedures in Internet Accessing issued by the Ministry of Public Security in December 1997. The regulation defines "harmful information" and further lists five kinds of harmful activities regarding Internet usage, “ (1) Intruding in a computer information network or making use of network resources without authorization; (2) Canceling, altering or adding functions in a computer information network without authorization; (3) Canceling, altering or adding data and application software for the purpose of memory, processing, or transmission in a computer information network without authorization; (4) Intentionally producing, disseminating destructive software such as a computer virus; (5) Other activities that are harmful to the security of a computer information network.” (Item 6)

Enforcement

In December 1997, Public Security minister Zhu Entao released new regulations to be enforced by the ministry that inflict fines for 'defaming government agencies,' 'splitting the nation,' and leaking "state secrets." Violators could face a fine up to 15,000 Yuan ($1800). Banning appears mostly coordinated and ad hoc, with some sites blocked, yet similar sites allowed or even blocked in one city and allowed in another. The blocks have often been lifted for special occasions. For example, *The New York Times* was unblocked when reporters in a private interview with Jiang Zemin specifically asked about the block and he replied that he would look into the matter. During the APEC summit in Shanghai during 2001, normally-blocked media sources such as CNN, NBC, and the *Washington Post* became accessible. Since 2001, the content controls have been further relaxed on a permanent basis, and all three of the sites previously mentioned are now accessible from mainland China. However, access to the New York Times was briefly re-blocked as of 20 December 2008, although it has been accessible for the first months of 2009 as of 17 May. The Chinese-language service of BBC News is still blocked.

Section Five of the Computer Information Network and Internet Security, Protection, and Management Regulations approved by the State Council on 11 December 1997 states the following:

No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information:

1. Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations;
2. Inciting to overthrow the government or the socialist system;
3. Inciting division of the country, harming national unification;
4. Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;
5. Making falsehoods or distorting the truth, spreading rumors, destroying the order of society;
6. Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder;
7. Terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;
8. Injuring the reputation of state organizations;
9. Other activities against the Constitution, laws or administrative regulations.

Golden Shield Project

The **Golden Shield Project** (Chinese: 金盾工程; Chinese: jīndùn gōngchéng) is owned by the Ministry of Public Security of the People's Republic of China (MPS). It started in 1998, began processing in November 2003, and the first part of the project passed the national inspection on 16 November 2006 in Beijing. According to MPS, its purpose is to construct a communication network and computer information system for police to improve their capability and efficiency. According to China Central Television (CCTV), by 2002 the preliminary work of the Golden Shield Project had cost US$800 million (equivalent to RMB 6,400 million or €640 million).

The Golden Shield Project is part of what is sometimes known outside of mainland China as the **Great Firewall of China** (in reference both to its role as a network firewall and to the ancient Great Wall of China). The system blocks content by preventing IP addresses from being routed through. It consists of standard firewalls and proxy servers at the Internet gateways. The system also selectively engages in DNS poisoning when particular sites are requested. The government does not appear to be systematically examining Internet content, as this appears to be technically impractical.

Researchers at the University of California, Davis and at the University of New Mexico said that the Great Firewall is not a true firewall since banned material is sometimes able to pass through several routers or through the entire system without being blocked.

Legislation

In September 2000, the State Council Order No. 292 created the first content restrictions for Internet content providers. China-based Web sites cannot link to overseas news Web sites or distribute news from overseas media without separate approval. Only “licensed

print publishers" have the authority to deliver news online. Non-licensed Web sites that wish to broadcast news may only publish information already released publicly by other news media. These sites must obtain approval from state information offices and from the State Council Information Agency. Article 11 of this order mentions that "content providers are responsible for ensuring the legality of any information disseminated through their services".

Article 14 gives Chinese officials full access to any kind of sensitive information they wish: " [...] an IIS provider must keep a copy of its records for 60 days and furnish them to the relevant state authorities upon demand in accordance to the law." Finally, article 15 defines what information must be restricted: "IIS providers shall not produce, reproduce, release, or disseminate information that: [...] endangers national security, [...] is detrimental to the honor of the state, [...] undermines social stability, the state's policy towards religion, [...] other information prohibited by the law or administrative regulations".

Censored content

Research into mainland Chinese Internet censorship has shown that censored websites included, before the 2008 Summer Olympics:

- Websites related to the persecuted Falun Gong spiritual practice
- News sources that often cover some topics such as police brutality, Tiananmen Square protests of 1989, freedom of speech and democracy sites. These sites include Voice of America, BBC News, and Yahoo! Hong Kong
- Media sites which may include unregulated content, social commentary or political commentary censored by the PRC.
- Sites hosted by Taiwan's government and major newspaper and television media and other sites with information on Taiwanese independence
- Web sites that contain obscenity, pornography, or criminal activity.
- The website of the separatist Central Tibetan Administration and of the "Voice of Tibet", an India-based dissident radio organization.
- "Nine Commentaries" or the nine articles that were published by theepochtimes.com that comment on the Chinese Communist Party

From the above list, the websites of BBC News, Yahoo! Hong Kong and the Voice of America were later unblocked (as observed on 17 August 2008). However, Voice of America and Yahoo! Hong Kong returned to their blocked status later on (as observed on 14 December 2009).

In the second half of 2009 the social networking sites Facebook and Twitter were blocked, presumably because of containing social or political commentary (similar to LiveJournal in the above list). An example is the commentary on the deadly riots in Xinjiang in July 2009. Another reason suggested for the block is that activists can utilize them to organize themselves.

Blocked websites are indexed to a lesser degree, if at all, by some Chinese search engines, such as Baidu and Google China. This sometimes has considerable impact on search results. According to a Harvard study, at least 18,000 websites are blocked from within mainland China. According to *The New York Times*, Google has set up computer systems inside China that try to access Web sites outside the country. If a site is inaccessible, then it is added to Google China's blacklist. However, once (if) unblocked, the websites will be reindexed.

Green Dam Youth Escort

A notice issued by the Ministry of Industry and Information Technology on 19 May stated that, as of 1 July 2009, manufacturers must ship machines to be sold in mainland China with the Green Dam software, and that manufacturers are required to report the number of machines shipped with the software to the government. The official statement claimed its objective was "to build a green, healthy, and harmonious online environment, and to avoid the effects on and the poisoning of our youth's minds by harmful information on the internet".

A senior official of the Internet Affairs Bureau of the State Council Information Office said the software's only purpose was "to filter pornography on the Internet". Foreign ministry official, Qin Gang said the internet had always been open in China and that the government's administration of it to prevent the spread of harmful information was in accordance with the law. The general manager of Jinhui, which developed Green Dam, said: "Our software is simply not capable of spying on Internet users, it is only a filter."

Human rights advocates and internet users in China have been especially critical, saying that while the software is ostensibly aimed at protecting users against pornography on the web, it "is really a thinly concealed attempt by the government to expand censorship". Online polls conducted on Sina, Netease, Tencent and Sohu revealed overwhelming (>70%) rejection of the software by netizens. A poll conducted by the *Southern Metropolis Daily* showed similar results.

On 10 June, the Publicity Department of the Communist Party of China Central Committee issued an instruction requiring the Chinese media to stop publishing questioning or critical opinions. The instruction also required online forums to block and remove "offensive speech evolved from the topic" promptly. Xinhua later commented that "support [for Green Dam] largely stems from end users, opposing opinions primarily come from a minority of media outlets and businesses".

On 14 August 2009, Li Yizhong, minister of industry and information technology, announced that computer manufacturers and retailers were no longer obliged to ship the software with new computers for home or business use, but that schools, internet cafes and other public use computers would still be required to run the software.

Political censorship

July 2009 Ürümqi riots

Government censors disabled keyword searches for "Urumqi", and blocked access to Facebook and Twitter as well as local alternatives Fanfou and Youku. Chinese news sites mainly fed from *Xinhua* news service for updates about the rioting in Urumqi, comments features on websites were disabled on some stories to prevent negative posts about the lack of news. Internet connections in Urumqi were reportedly down. Many unauthorized postings on local sites and Google were said to have been "harmonised" by government censors, and emails containing terms related to the riots were blocked or edited to prevent discord. Nevertheless, images and video footage of the demonstrations and rioting were soon found posted on Twitter, YouTube and Flickr.

20th anniversary of Tiananmen Square protests

"*For reason which everyone knows, and to suppress our extremely unharmonious thoughts, this site is voluntarily closed for technical maintenance between 3 and 6 June 2009...*" Dusanben.com (translation)

Coinciding with the twentieth anniversary of the government suppression of the pro-democracy protests in Tiananmen Square, the government ordered internet portals, fora and discussion groups to shut down their servers for maintenance between 3 and 6 June.

> “
>
> In order to improve the internet content and provide a healthy environment for our netizens, we have designated 3 to 6 June as the national server maintenance day. This move is widely supported by the public
>
> ”
>
> –Chinese censors, *South China Morning Post*

The Guardian reported that in excess of 300 Chinese sites had "posted increasingly blasé maintenance messages on the anniversary". A number of websites, such as Fanfou and WordKu.com, made a veiled protest at state censorship by referring to the date

sarcastically as "Chinese Internet Maintenance Day". The day before the mass shut-down, Chinese users of Twitter, Hotmail and Flickr, among others, reported a widespread inability to access these services.

2008 Olympics

IOC agreement

Initially, the Chinese government, the IOC and Jacques Rogge had stated that Internet access would not be censored at the Olympic Village press center. However, journalists that arrived at the press center after its opening on 25 July found that sites containing politically sensitive matter were inaccessible and learned that the IOC had quietly agreed to "some of the limitations." IOC press chief Kevan Gosper admitted that, "I regret that it now appears BOCOG has announced that there will be limitations on Web site access during Games time. I also now understand that some IOC officials negotiated with the Chinese that some sensitive sites would be blocked on the basis they were not considered Games related." Foreign media was not informed about this private agreement, and IOC press chief Kevan Gosper apologized to journalists for giving the impression that Internet access during the Olympics would be completely unrestricted. Furthermore, on 31 July 2008, the BOCOG Chinese spokesman, Sun Weide, indicated that the media will have "convenient and sufficient" access to the Internet. However, he also said that the government won't allow the spread of any information on the internet that is forbidden by Chinese law or harms national interests.

Partial censorship

The censorship at the press center added to a growing skepticism about the claims of the government that it would improve its record on human rights. The "broken promise" was condemned by Reporters Without Borders who pointed out that about 20,000 foreign journalists would be directly affected. A pre-Olympics crackdown by the China Internet Illegal Information Reporting Centre on “illicit” websites, temporarily shut down Qingdaonews.com, 21CN, Sichuan online, Shenzhen online, Tom online, and cjn.cn. Some websites and blogs with politically sensitive content, such as bulletin board services on tecn.cn and Xici.net, have been blocked.

On 1 August 2008, Reuters reported that Internet restrictions would be lifted for reporters covering the Olympics. Beginning 1 August, in response to international criticism, some previously-blocked websites became accessible, including Human Rights Watch and Amnesty International. Many websites related to Falun Gong and Tibet remained blocked. The BBC's Chinese-language site was intermittently accessible and blocked. As of 5 August, the BBC's English website previously barred, remain open, if slow to load - as does the Hong Kong-based Apple Daily. However the Chinese version was blocked again in December 2008.

Reporters Without Borders subsequently confirmed that its website, except for the Chinese version, was accessible for the first time in China since 2003. The Chinese

version of the website is still blocked. While some previously-censored foreign websites were accessible during the Olympics, Reporters Without Borders claims that there has been increased restriction of domestic websites and online activity, including the popular internet chatting service "QQ". On 2 August 2008, the Associated Press reported that although Chinese organizers unblocked some sites at the request of the IOC, others remained censored for journalists covering the Summer Games. Even though Chinese officials and high-ranking IOC members have repeatedly said there would be no censorship on the Internet for accredited journalists covering the games, many sites the Chinese government objects to, for example, the spiritual movement Falun Gong, are blocked. The sites being blocked seem to change daily. Some key words always draw blank screens. Sites that host thousands of blogs are also routinely blocked. As of 4 August, Human Rights in China and websites affiliated with Tibetan independence and the outlawed spiritual movement Falun Gong, remained inaccessible inside and outside of Olympic venues.

Access to Apple, Inc.'s online iTunes Store was blocked in China after it emerged that Olympic athletes had been downloading a pro-Tibetan album in a subtle act of protest. However, this action lasted only for a short time before it was revoked by the government. The album, Songs for Tibet, was produced by a group called The Art of Peace Foundation, and features 20 tracks from well-known singers and songwriters including Sting, Moby, and Suzanne Vega.

Crackdown on Internet activists

In 2001, Wang Xiaoning and other Chinese activists were arrested and sentenced to 10 years in prison for using a Yahoo email account to post anonymous writing to an Internet mailing list, which Yahoo, after pressure from the Chinese government eventually blocked. However, with the help of the World Organization for Human Rights, Wang and Shi Tao, another online activist sued Yahoo, accusing the Internet provider of abetting the torture of pro-democracy writers by providing information that allowed the Chinese government to identify them.

On 23 July 2008, the family of Liu Shaokun was notified that he had been sentenced to one year re-education through labor for “inciting a disturbance”. A teacher in Sichuan province, he had taken photographs of collapsed schools and posted these photos online.

On 18 July 2008, Huang Qi was formally arrested on suspicion of illegally possessing state secrets. Huang had spoken with the foreign press and posted information on his website about the plight of parents who had lost children in collapsed schools.

Locking data centers

The Ministry of Industry and Information Technology of the People's Republic of China ordered all ISPs to lock down their data centers from 1–25 August 2008. During this time no one could enter data centers to do maintenance. Sites with illegal information were blocked automatically. Authorities stated it was to ensure data security, to prevent hostile

personnel from entering data centers and adding illegal information.
ISP/IDCs have sent "lockdown notices" to customers.
Companies have received orders stating that from 1–25 August 2008:

1. Customers will not be able to enter data centers.
2. Customers will not able to add new hardware.
3. Any sites with illegal information will be blocked automatically, and site owners will not be able to request unblocking as they normally can.

In customers' interests, companies have suggested:

1. Customers should manage their sites carefully. Forums mediators should check any new posts before publishing, and customers should shut down all interactive services including forums, because sites will be blocked if customers fail to filter out illegal information.
2. Avoid maintenance.
3. Reduce promotions.
4. Contact the company as soon as possible if a customer wants to add new hardware.

Self-censorship

Internet censorship in the PRC has been called "a panopticon that encourages self-censorship through the perception that users are being watched." The enforcement (or threat of enforcement) of censorship creates a chilling effect where individuals and businesses willingly censor their own communications to avoid legal and economic repercussions. Professor Yantao BI reported on 30 October 2008 that some websites in mainland China have already imposed the controversial true-name registration policy.

Search engines

One part of the block is to filter the search results of certain terms on Chinese search engines. These Chinese search engines include both international ones (for example, yahoo.com.cn and Google China) as well as domestic ones (for example, Baidu). Attempting to search for censored keywords in these Chinese search engines will yield few or no results. Google.cn will display the following at the bottom of the page: "According to the local laws, regulations and policies, part of the searching result is not shown."

In addition, a connection containing intensive censored terms may also be closed by The Great Firewall, and cannot be reestablished for several minutes. This affects all network connections including HTTP and POP, but the reset is more likely to occur during searching.

Before the search engines censored themselves, many search engines had been blocked, namely Google and AltaVista. Technorati, a search engine for blogs, has been blocked.

Different search engines implement the mandated censorship in different ways. For example, the search engine Bing is reported to censor search results from searches conducted in simplified Chinese characters (used in the PRC), but not in traditional Chinese characters (used in Taiwan and elsewhere). Google search results depend on whether the search is done using the google.cn search engine, based in mainland China, or using Google search engines based outside of China; the google.cn search results include a small note stating that some results are not being shown if pages on the blocked list come up on the search.

CERNET

Several Bulletin Board Systems in universities were closed down or restricted public access since 2004, including the SMTH BBS and the YTHT BBS.

Local businesses

Although blocking foreign sites has received much attention in the West, this is actually only a part of the PRC effort to censor the Internet. The ability to censor content providers within mainland China is much more effective, as the ISPs and other service providers are restricting customers' actions for fear of being found legally liable for customers' conduct. The service providers have assumed an editorial role with regard to customer content, thus became publishers, and legally responsible for libel and other torts committed by customers.

Although the government does not have the physical resources to monitor all Internet chat rooms and forums, the threat of being shut down has caused Internet content providers to employ internal staff, colloquially known as "big mamas", who stop and remove forum comments which may be politically sensitive. In Shenzhen, these duties are partly taken over by a pair of police-created cartoon characters, Jingjing and Chacha, who help extend the online 'police presence' of the Shenzhen authorities. These cartoons spread across the nation in 2007 reminding internet users that they are being watched and should avoid posting 'sensitive' or 'harmful' material on the internet.

However, Internet content providers have adopted some counter-strategies. One is to post politically sensitive stories and remove them only when the government complains. In the hours or days in which the story is available online, people read it, and by the time the story is taken down, the information is already public. One notable case in which this occurred was in response to a school explosion in 2001, when local officials tried to suppress the fact the explosion resulted from children illegally producing fireworks. By the time local officials forced the story to be removed from the Internet, the news had already been widely disseminated.

In addition, Internet content providers often replace censored forum comments with white space which allows the reader to know that comments critical of the authorities had been submitted, and often to guess what they might have been.

In July 2007, the city of Xiamen announced it would ban anonymous online postings after text messages and online communications were used to rally protests against a proposed chemical plant in the city. Internet users will be required to provide proof of identity when posting messages on the more than 100,000 Web sites registered in Xiamen.

Some hotels in China are also advising internet users to obey local Chinese internet access rules by leaving a list of internet rules and guidelines near the computers. These rules, among other things, forbid linking to politically unacceptable messages, and inform internet users that if they do, they will have to face legal consequences.

In September 2007, some data centers were shut down indiscriminately for providing interactive features such as blogs and forums. CBS reports an estimate that half the interactive sites hosted in China were blocked.

International corporations

One controversial issue is whether foreign companies should supply equipment to the PRC government which may assist in the blocking of sites. Some argue that it is wrong for companies to profit from censorship including restrictions on freedom of the press and freedom of speech. Others argue that equipment being supplied- from companies such as the American based Cisco Systems Inc.- is standard Internet infrastructure equipment and that providing this sort of equipment actually aids the flow of information, and that the PRC is fully able to create its own infrastructure without Western help. By contrast, human rights advocates such as Human Rights Watch and media groups such as Reporters Without Borders argue that if companies stopped contributing to the authorities' censorship efforts, the government could be forced to change.

A similar dilemma is faced by foreign content providers such as Yahoo! AOL, and Skype who abide by PRC government wishes, including having internal content monitors, in order to be able to operate within mainland China. Also, in accordance with mainland Chinese laws, Microsoft began to censor the content of its blog service Windows Live Spaces, arguing that continuing to provide Internet services is more beneficial to the Chinese. Michael Anti, a Chinese journalist whose blog on Windows Live Spaces was removed by Microsoft, agreed that the Chinese are better off with Windows Live Spaces than without it.

The Chinese version of MySpace, launched in April 2007, has many censorship-related differences from other international versions of the service. Discussion forums on topics such as religion and politics are absent and a filtering system that prevents the posting of content about Taiwan independence, the Dalai Lama, Falun Gong, and other "inappropriate topics" has been added. Users are also given the ability to report the "misconduct" of other users for offenses including "endangering national security, leaking state secrets, subverting the government, undermining national unity, spreading rumors or disturbing the social order."

Additionally, reporters in the western media have also suggested that China's internet censorship of foreign websites may also be a means of forcing mainland Chinese users to rely on China's own e-commerce industry, thus self-insulating their economy from the dominance of international corporations.

Reactions

Legal action

On 9 May 2007, Mr. Yetaai (冬劲) sued Shanghai Telecom, a sub-company of China Telecom, because one of his sites was blocked from access in China. He then took a series of steps including raising maintenance request and notarization. His lawsuit was accepted by Pu Dong Court, Shanghai. Mr. Yetaai reported it through his online diary (English). He also raised an item for online ticketing through an article on Digg.

Liberalization of sexually oriented content

Although restrictions on political information remain strong, several sexually oriented blogs began appearing in early 2004. Women using the web aliases Muzi Mei (木子美) and Zhuying Qingtong (竹影青瞳) wrote online diaries of their sex lives and became minor celebrities. This was widely reported and criticized in mainland Chinese news media, and several of these bloggers' sites have since been blocked in China to this day. This coincided with an artistic nude photography fad (including a self-published book by dancer Tang Jiali) and the appearance of pictures of minimally clad women or even topless photos in a few mainland Chinese newspapers, magazines and websites. Many dating and "adult chat" sites, both Chinese and foreign, have been blocked. Some, however, continue to be accessible although this appears to be due more to the Chinese government's ignorance of their existence than any particular policy of leniency.

Corporate responsibility

On 7 November 2005 an alliance of investors and researchers representing 26 companies in the U.S., Europe and Australia with over US $21 billion in joint assets announced that they were urging businesses to protect freedom of expression and pledged to monitor technology companies that do business in countries violating human rights, such as China. On 21 December 2005 the UN, OSCE and OAS special mandates on freedom of expression called on Internet corporations to "work together ... to resist official attempts to control or restrict use of the Internet." Google finally responded when attacked by hackers rumoured to be hired by the Chinese government by threating to pull out of China (Newsweek)

Technical efforts at breaking through

The firewall is largely ineffective at preventing the flow of information and is rather easily circumvented by determined parties by using proxy servers outside the firewall.

VPN and SSH connections to outside mainland China are not blocked, so circumventing all of the censorship and monitoring features of the Great Firewall of China is trivial for those who have these secure connection methods to computers outside mainland China available to them.

Since free hosting blog services like Blogger and Wordpress.com frequently face blockage, bloggers and webmasters aiming for an audience in China often debate merits of the various paid hosting services. Some China-focused services explicitly offer to change a blog's IP address within 30 minutes if it is blocked by the authorities.

Psiphon is a software project designed by University of Toronto's Citizen Lab under the direction of Professor Ronald Deibert, Director of the Citizen Lab. Psiphon is a circumvention technology that works through social networks of trust and is designed to help Internet users bypass content-filtering systems set up by governments.

The Tor website is blocked although the Tor network isn't, making Tor (in conjunction with Privoxy) an effective tool for circumvention of the censorship controls if one can acquire it. Tor maintains a public list of entry nodes, so the authorities could easily block it if they had the inclination. According to the sections 6.4 and 7.9, Tor is vulnerable to timing analysis by Chinese authorities, so it allows a breach of anonymity. Thus for the moment, Tor allows uncensored downloads and uploads, although no guarantee can be made with regard to freedom from repercussions. Since September 25, 2009, about 80% of the public relays are blocked by IP address and TCP port combination but Tor users are still connecting to the network through non-public relays (bridges).

As an alternative to Tor, there are various HTTP/HTTPS Tunnel Services.

It was common in the past to use Google's cache feature to view blocked websites. However, this feature of Google seems to be under some level of blocking, as access is now erratic and does not work for blocked websites. Currently the block is mostly circumvented by using proxy servers outside the firewall, and is not difficult to carry out for those determined to do so. Some well-known proxy servers have also been blocked.

Some Chinese citizens used the Google mirror elgooG after China blocked Google. It is believed that elgooG survived the Great Firewall of China because the firewall operators thought that elgooG was not a fully functional version of Google. (This information is out of date, referring to an early blockade of Google in 2002)

There are several techniques (websites and programs) that may be used to browse blocked sites. These include:

- Ultrareach
- Gollum
- picidae
- Freegate
- Garden and GTunnel by Garden Networks

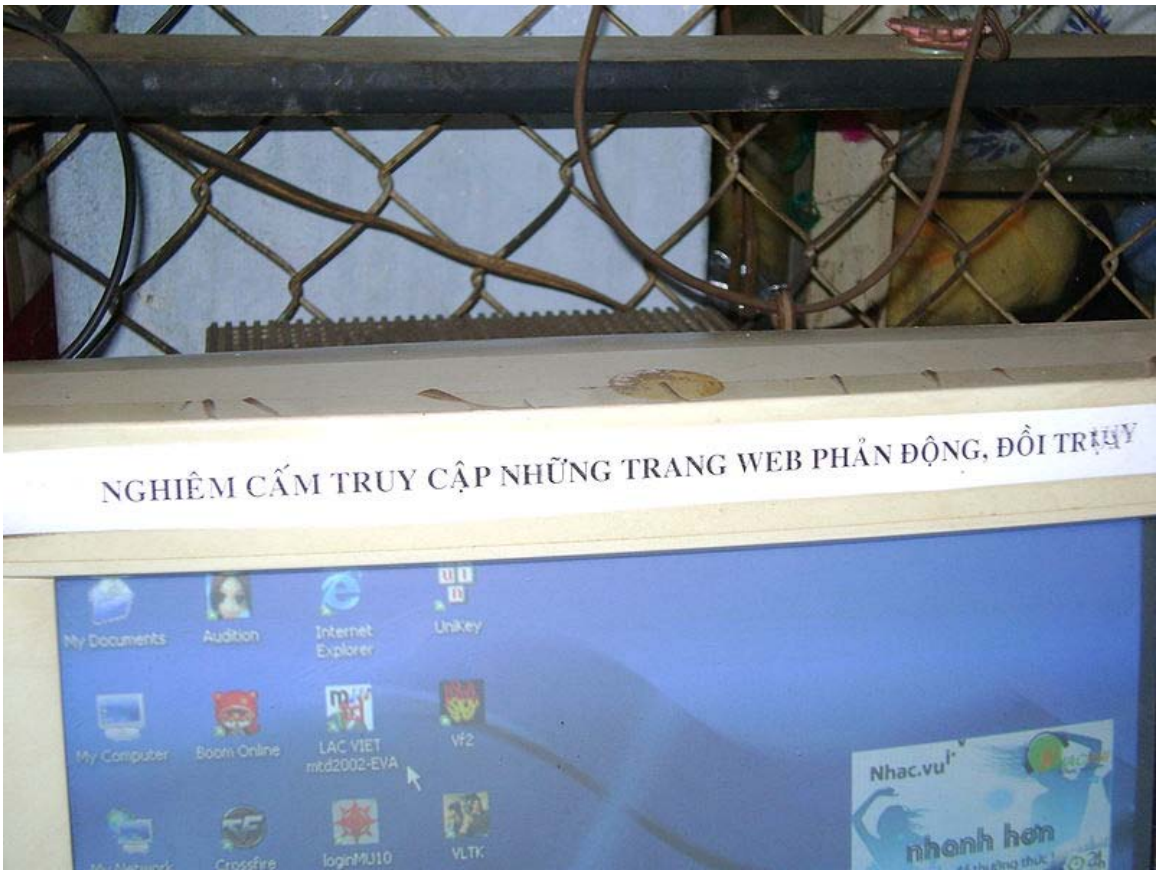
Societal and cultural evasion

The Baidu 10 Mythical Creatures, initially a humorous hoax, has become a popular and widespread internet meme in China. These hoaxes, ten in number, reportedly originated in response to increasingly pervasive and draconian online censorship and have become an icon of citizens' resistance to censorship.

The State Administration of Radio, Film, and Television issued a directive on 30 March 2009 to highlight 31 categories of content prohibited online, including violence, pornography and content which may "incite ethnic discrimination or undermine social stability". Many netizens believe the instruction follows the official embarrassment over the "Grass Mud Horse" and the "River Crab". Industry observers believe that the move was designed to stop the spread of parodies or other comments on politically sensitive issues in the runup to the anniversary of the 4 June Tiananmen Square protests.

Chapter 10

Internet Censorship in Vietnam



A sign above a computer monitor in an Internet cafe reminding patrons that they are forbidden from accessing sites with "reactionary" or "depraved" content

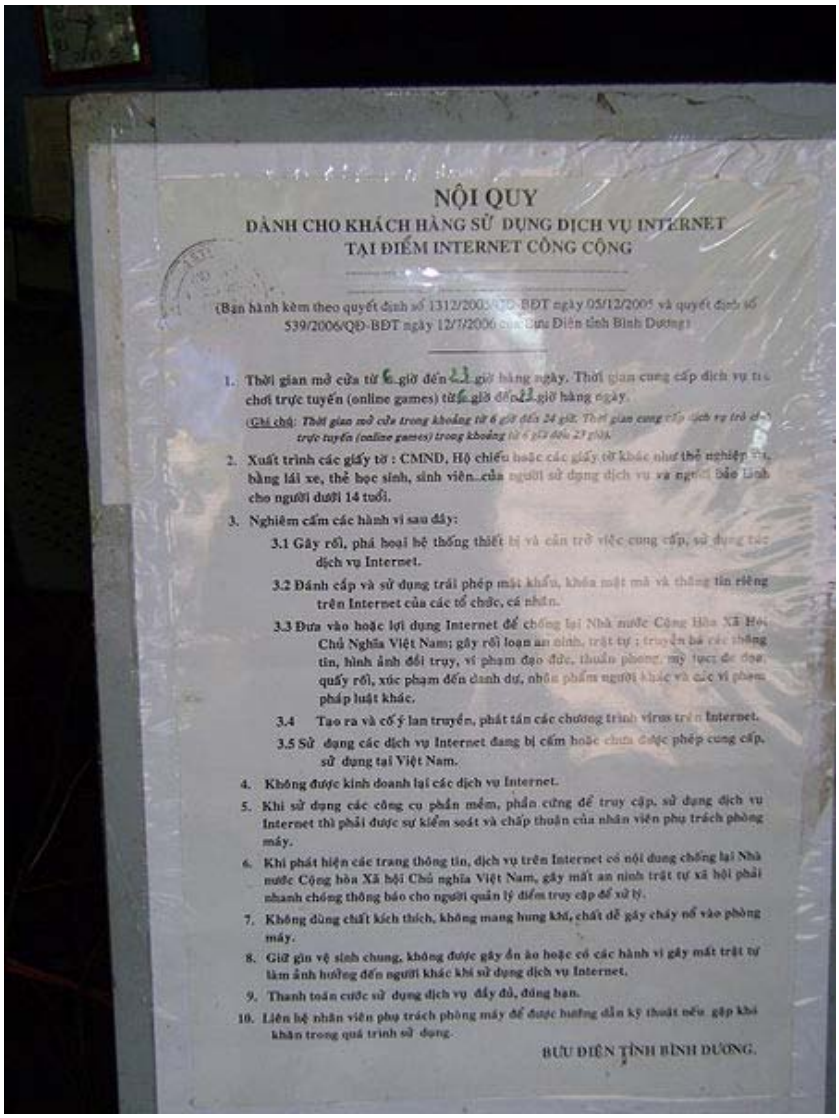
Vietnam extensively **regulates Internet access** to its citizens, using both legal and technical means. The collaborative project OpenNet Initiative classifies Vietnam's level of online political censorship to be "pervasive" while Reporters without Borders considers Vietnam one of 15 "internet enemies". While the government of Vietnam claims to safeguard the country against obscene or sexually-explicit content through its blocking efforts, much of the filtered sites contain politically or religiously sensitive materials that might undermine the Communist Party's hold on power. Amnesty

International reported many instances of Internet activists being arrested for their online activities.

Censored content

Censorship can usually be bypassed by using either The Onion Router or Google's "Cached" feature.

Subversive content



NỘI QUY

DÀNH CHO KHÁCH HÀNG SỬ DỤNG DỊCH VỤ INTERNET
TẠI ĐIỂM INTERNET CÔNG CỘNG

(Ban hành kèm theo quyết định số 1312/2005/QĐ-BĐT ngày 05/12/2005 và quyết định số 539/2006/QĐ-BĐT ngày 12/7/2006 của Bưu Điện tỉnh Bình Dương)

1. Thời gian mở cửa từ 6 giờ đến 23 giờ hàng ngày. Thời gian cung cấp dịch vụ trò chơi trực tuyến (online games) từ 6 giờ đến 23 giờ hàng ngày.
   (Ghi chú: *Thời gian mở cửa trong khoảng từ 6 giờ đến 24 giờ. Thời gian cung cấp dịch vụ trò chơi trực tuyến (online games) trong khoảng từ 6 giờ đến 23 giờ.*
2. Xuất trình các giấy tờ : CMND, Hộ chiếu hoặc các giấy tờ khác như thẻ nghiệp vụ, bằng lái xe, thẻ học sinh, sinh viên...của người sử dụng dịch vụ và người bảo lãnh cho người dưới 14 tuổi.
3. Nghiêm cấm các hành vi sau đây:
   3.1 Gây rối, phá hoại hệ thống thiết bị và cản trở việc cung cấp, sử dụng các dịch vụ Internet.
   3.2 Đánh cắp và sử dụng trái phép mật khẩu, khóa mật mã và thông tin riêng trên Internet của các tổ chức, cá nhân.
   3.3 Đưa vào hoặc lợi dụng Internet để chống lại Nhà nước Cộng Hòa Xã Hội Chủ Nghĩa Việt Nam; gây rối loạn an ninh, trật tự ; truyền bá các thông tin, hình ảnh đồi trụy, vi phạm đạo đức, thuần phong, mỹ tục để đe dọa, quấy rối, xúc phạm đến danh dự, nhân phẩm người khác và các vi phạm pháp luật khác.
   3.4 Tạo ra và cố ý lan truyền, phát tán các chương trình virus trên Internet.
   3.5 Sử dụng các dịch vụ Internet đang bị cấm hoặc chưa được phép cung cấp, sử dụng tại Việt Nam.
4. Không được kinh doanh lại các dịch vụ Internet.
5. Khi sử dụng các công cụ phần mềm, phần cứng để truy cập, sử dụng dịch vụ Internet thì phải được sự kiểm soát và chấp thuận của nhân viên phụ trách phòng máy.
6. Khi phát hiện các trang thông tin, dịch vụ trên Internet có nội dung chống lại Nhà nước Cộng hòa Xã hội Chủ nghĩa Việt Nam, gây mất an ninh trật tự xã hội phải nhanh chóng thông báo cho người quản lý điểm truy cập để xử lý.
7. Không dùng chất kích thích, không mang hung khí, chất dễ gây cháy nổ vào phòng máy.
8. Giữ gìn vệ sinh chung, không được gây ồn ào hoặc có các hành vi gây mất trật tự làm ảnh hưởng đến người khác khi sử dụng dịch vụ Internet.
9. Thanh toán cước sử dụng dịch vụ đầy đủ, đúng hạn.
10. Liên hệ nhân viên phụ trách phòng máy để được hướng dẫn kỹ thuật nếu gặp khó khăn trong quá trình sử dụng.

BƯU ĐIỆN TỈNH BÌNH DƯƠNG.

A list of regulations posted at an Internet cafe in Ho Chi Minh City, among the listed rules are those forbidding patrons from accessing sites with subversive or pornographic content.

OpenNet research found that blocking is concentrated on websites with contents about overseas political opposition, overseas and independent media, human rights, and

religious topics. Proxies and circumvention tools, which are illegal to use, are also frequently blocked.

The majority of blocked websites are specific to Vietnam: those written in Vietnamese or dealing with issues related to Vietnam. Sites not specifically related to Vietnam or only written in English are rarely blocked. For example, the Vietnamese language version of the website for Radio Free Asia was blocked by both tested ISPs while the English-language version was only blocked by one. While only the website for the human rights organization Human Rights Watch was blocked in the tested list of global human rights sites, many Vietnamese-language sites only tangentally or indirectly critical of the government were blocked as well as sites strongly critical of the government.

Social networking

The popular social networking website Facebook has about 1 million users in Vietnam and its user base has been growing quickly after the website added a Vietnamese-language interface. During the week of November 16, 2009, Vietnamese Facebook users reported being unable to access the website. Access had been intermittent in the previous weeks and there were reports of technicians ordered by the government to block access to Facebook.

A supposedly official decree dated August 27, 2009 was earlier leaked on the Internet, but its authenticity has not been confirmed. The Vietnamese government denied deliberately blocking access to Facebook and the Internet service provider FPT said that it is working with foreign companies to solve a fault blocking to Facebook's servers in the United States.

Blogging

In Vietnam, Yahoo! 360° is a popular blogging service. After the government crackdown on journalists reporting on corruption in mid-2008, many blogs covered the events, often criticizing the government action. In response, the Ministry of Information proposed new rules that would restrict blogs to personal matters.

Chapter 11

Censorship of YouTube

YouTube logo

YouTube, the third-most visited website in the world (according to Alexa Internet), has been censored several times in some countries since its inception.

As of November 2010, countries with standing national bans on YouTube are China, Iran, Libya, Tunisia, and Turkmenistan.

Worldwide

Windows Live Messenger

On May 10, 2008, Microsoft temporarily banned functional YouTube links from its Live Messenger Service (although the ban was lifted as of 21:30 GDT). Microsoft never commented on the blocking. The sending of any functional link starting with either http:// or www. with the string "youtube.com" contained within it returned an error message saying "The following message could not be delivered to all recipients: (original message here)." Coincidentally, or not, Messenger TV, a new video service provided by Microsoft was scheduled for release the same week.

By educational institutions

Brigham Young University

Some U.S. Colleges are also blocking YouTube access. Brigham Young University, a private university run by the LDS (Mormon) Church had blocked YouTube access in the past, but this policy was changed in June 2009.

Southern California Institute of Architecture

The graduate and undergraduate student bodies of the Southern California Institute of Architecture are denied access to YouTube and other common video sites such as Google Video, without regard for their educational content. The administration cites bandwidth concerns to legitimize this prohibition.

In NSW

Youtube has been blocked at all schools routed through the DET's network, but it may be accessed via a proxy. Teachers may show educational videos.

K-12 Schools

Many K-12 schools in the United States and Canada block access to YouTube due to sexual, violent, and unusual content, and due to bandwidth consumption. Some schools do allow it for educational purposes.

In the UK

YouTube and other video streaming websites are also blocked from access in schools across the UK to 'avoid distraction from work'. This only applies to students, as in some schools some teachers are allowed access to YouTube to show videos which are educational. This is done through the use of proxy censor systems through the council's Internet provision, which most schools receive through.

In most East Midlands schools, including RBEC, YouTube is blocked using filtering made available by the East Midlands Broadband Company.

Some schools across the UK, however, allow access to YouTube for the students but they are only permitted to watch videos considered to be appropriate. They are not to log into their accounts or upload videos.

UCTI Malaysia

YouTube has been blocked from access to reduce the likelihood of students clogging up the bandwidth.

By businesses

Hospital Corporation of America

Hospital Corporation of America blocks access to YouTube on its computers. This may be due to bandwidth consumption.

By country

Armenia

Following the disputed February 2008 presidential elections, the Armenian Government temporarily blocked internet users from YouTube. The Armenian opposition had used the website to publicize video of police and military brutality carried out against anti-government protesters.

Brazil

YouTube is being sued by Brazilian model and MTV VJ Daniela Cicarelli (better known as Ronaldo's ex-fiancée) on the grounds that the site makes available video footage made by a paparazzo in which she and her boyfriend are having sex on a Spanish beach. The lawsuit requires that YouTube be blocked in Brazil until all copies of the video are removed. On Saturday, January 6, 2007, a legal injunction ordered that filters be put in place to prevent users in Brazil from accessing the website.

The effectiveness of the measure has been questioned, since the video is available not only on YouTube, but also on other sites as part of an Internet phenomenon. On Tuesday, January 9, 2007, the same court overturned their previous decision, ordering the filters removed, although the footage itself remained forbidden, but without technical support for its blockage.

Bangladesh

In March 2009, YouTube was blocked in Bangladesh after a recording of a meeting between the prime minister and army officers was posted revealing anger by the military on how the government was handling a mutiny by border guards in Dhaka.The block is lifted at present.

Indonesia

On April 1, 2008, Indonesian information minister, Muhammad Nuh, wrote to YouTube asking them to remove a controversial Dutch film, Fitna, made by Dutch right-wing politician, Geert Wilders. The Indonesian government allowed two days for the removal of the video, or YouTube would be blocked in Indonesia. On April 4, 2008, Muhammad Nuh asked all Internet service providers to block the access to YouTube. On April 5, 2008, YouTube was blocked for testing by one ISP. Finally, on April 8, YouTube, along

with MySpace, Metacafe, RapidShare, Multiply, Liveleak, and Fitna's official site, were blocked in Indonesia. YouTube's ban was lifted on April 10. There may still be some blocking in May 2008 according to local inhabitants.

Iran

On December 3, 2006, Iran blocked YouTube, along with several other sites, after declaring them "immoral". The YouTube ban came after a video was posted online that appears to show an Iranian soap opera star having sex. The block was later lifted and then reinstated after the 2009 presidential election.

Libya

On 24 January 2010, Libya indefinitely blocked YouTube after it featured videos of demonstrations in the Libyan city of Benghazi by families of detainees who were killed in Abu Salim prison in 1996, as well as videos of family members of Libyan leader Moamer Kadhafi at parties. The ban was condemned by Human Rights Watch.

Morocco

On May 25, 2007, the state-owned Maroc Telecom blocked all access to YouTube. There were no reasons given as to why YouTube was blocked, but speculations are that it might have something to do with some posted pro-separatist group Polisario clips (Polisario being the Western Sahara independence movement) or because of some videos criticizing King Mohammed VI. The government ban did not concern the other two private internet providers, Wana and Méditel. YouTube became accessible again on May 30, 2007, after *Maroc Telecom* unofficially announced that the denied access to the website was a mere "technical glitch".

Pakistan

YouTube was blocked in Pakistan following a decision taken by the Pakistan Telecommunication Authority on February 22, 2007 because of the number of "non-Islamic objectionable videos." One report specifically names Fitna, a controversial Dutch film, as the basis for the block. Pakistan, an Islamic republic, ordered its ISPs to block access to YouTube "for containing blasphemous web content/movies." Blasphemy law in Pakistan calls for life imprisonment or death. Router misconfiguration by one Pakistani ISP effectively blocked YouTube access worldwide for several hours on February 24, 2007.

This follows increasing unrest in Pakistan by Islamic extremists over the reprinting of the Jyllands-Posten Muhammad cartoons which depict satirical Criticism of Islam. However, it has been suggested by some Pakistani vigilante web sites and electoral process watchdog groups that the block was imposed largely to distract viewers from videos alleging vote-rigging by the ruling MQM party in the recently concluded general elections. Allegations of suppressing vote-rigging videos by the Musharraf administration

are also being leveled by Pakistani bloggers, newspapers, media, and Pakistani anti-Musharraf opposition parties.

On February 26, 2007, the ban was lifted after the website had removed the objectionable content from its servers at the request of the government.

On 20 May 2010, on Everybody Draw Mohammed Day Pakistan again blocked the website in a bid to contain "blasphemous" material.

On May 31, 2010, the ban was lifted after the website had removed the objectionable content from its servers at the request of the government.

China

YouTube was blocked in the People's Republic of China, beginning on 15 October 2007, but later became unblocked.

However, due to it carrying video of soldiers beating monks and other Tibetans, YouTube has been blocked in Mainland China since 24 March 2009.

As of December 2010, YouTube is still being blocked in China.

Sudan

The Sudanese authorities blocked YouTube on April 21, 2010, following the recent presidential elections, and also blocked YouTube's owner Google. The block was in response to a YouTube video showing National Electoral Commission workers in official uniforms and a child in the Hamashkoreib region filling out voting strips and putting them into ballot boxes, with one of them expressing relief that the voting period had been extended for them to finish their work. Sudan had previously blocked YouTube temporarily in 2008 for unknown reasons.

Russia

The video claiming responsibility for the 2010 Moscow Metro bombings, which claimed 800,000 viewers in four days, was removed, along with all videos of Doku Umarov. Additionally, it turned out that over 300 videos from the Kavkaz Center were removed because of having "inappropriate content." Russia was blamed for having pressured Youtube to take such measures.

On July 28, 2010, a court in the city of Komsomolsk-on-Amur has ordered a local ISP to block access to youtube.com, along with web.archive.org and several websites offering books for downloads, citing extremist materials as the reason. Later this decision was revoked.

Thailand

In 2006, Thailand blocked access to YouTube for users with Thai IP addresses. Thai authorities identified 20 offensive videos and demanded that Google remove them before it would allow unblocking of all YouTube content.

During the week of March 8, 2007, YouTube was blocked in Thailand. Many bloggers believed the reason for the blocking was a posted video of former Prime Minister Thaksin Shinawatra's speech on CNN. The government did not confirm or provide reasons for the ban. YouTube became accessible again on March 10, 2007.

On the night of April 3, 2007, YouTube was again blocked in Thailand. The government cited a video on the site that it called "insulting" to King Bhumibol Adulyadej. However, the Ministry of Information and Communication Technology claimed that it would unblock YouTube in a few days, after websites containing references to this video are blocked instead of the entire website. Communications Minister Sitthichai Pokai-udom said, "When they decide to withdraw the clip, we will withdraw the ban." Shortly after this incident the internet technology blog Mashable was blocked from Thailand over the reporting of the YouTube clips in question. YouTube was unblocked on August 30, 2007, after YouTube reportedly agreed to block videos deemed offensive by Thai authorities.

On September 21, 2007, Thai authorities announced they were seeking a court order to block videos that had recently appeared on YouTube accusing Privy Council president Prem Tinsulanonda of attempting to manipulate the royal succession to make himself Thailand's king.

Tunisia

YouTube has been blocked in Tunisia since at least November 2, 2007, with a forged HTTP 404 error message appearing instead. The reasons for such an action are not immediately known, and no explanations have been given. YouTube is the second video site to display such messages.

Turkey

Turkish courts have banned YouTube between March 2007 and October 2010 (the first ban taking place between March 6 and March 9 of 2007) and thus users in Turkey could not access the site.

Türk Telekom first blocked YouTube in compliance with decision 2007/384 issued by the Istanbul 1st Criminal Court of Peace (*Sulh Ceza Mahkeme*) on 6 March 2007. The court decision was based on videos insulting Mustafa Kemal Atatürk in an escalation of what the Turkish media referred to as a "virtual war" of insults between Greek, Armenian and Turkish YouTube members. YouTube was sued for "insulting Turkishness" and access to the site was suspended pending the removal of the video. YouTube lawyers sent proof of the video's removal to the Istanbul public prosecutor and access was restored on

March 9, 2007. However, other videos similarly deemed insulting were repeatedly posted, and several staggered bans followed, issued by different courts:

- the Sivas 2nd Criminal Court of Peace on 18 September 2007 and again (by decision 2008/11) on 16 January 2008;
- the Ankara 12th Criminal Court of Peace on 17 January 2008 (decision 2008/55);
- the Ankara 1st Criminal Court of Peace on 12 March 2008 (decision 2008/251);
- the Ankara 11th Criminal Court of Peace on 24 April 2008 (decision 2008/468).
- the Ankara 5th Criminal Court of Peace on 30 April 2008 (decision 2008/599);
- again, the Ankara 1st Criminal Court of Peace on 5 May 2008 (decision 2008/402);
- again, the Ankara 11th Criminal Court of Peace on 6 June 2008 (decision 2008/624).

The block in accordance with court decision 2008/468 of the Ankara 11th Criminal Court of Peace issued on April 24, 2008, which cited that YouTube had not acquired a certificate of authorisation in Turkey, was not implemented by Türk Telekom until May 5, 2008.

Although YouTube was officially banned in Turkey, the website was still accessible by modifying connection parameters to use alternative DNS servers, and it was the sixth most popular website in Turkey according to Alexa records. Responding to criticisms of the courts' bans, the Prime Minister Recep Tayyip Erdoğan has famously stated "I do access the site. Go ahead and do the same." in November 2008.

In June 2010, Turkey's president Abdullah Gül used his Twitter account to express disapproval of the country's blocking of YouTube, which also affects access from Turkey to many Google services. Gül said he had instructed officials to find legal ways of allowing access.

Turkey lifted the ban on 30 October 2010, but the ban was reinstated on 3 November 2010.

Turkmenistan

On December 25, 2009, YouTube was blocked in Turkmenistan by the only ISP Turkmentelecom. Other web-sites such as LiveJournal were blocked, too.

United Arab Emirates

The UAE's telecom regulatory authority blocked YouTube in August 2006, with the Etisalat ISP in the UAE citing "presence of adult content on the website which is clearly against the religious, cultural, political and moral values of the UAE". Etisalat unblocked Youtube a month later.

Chapter 12

Internet Censorship in the United States and United Kingdom

Internet censorship in the United States

Internet censorship in the United States is the suppression of information published or viewed on the Internet in the United States. Personal Internet access in the US is not subject to technical censorship but can be penalized by law for violating the rights of others. Programs such as content-control software are sometimes used within institutions such as businesses, libraries, schools, and government offices. Though most online expression is protected by the First Amendment to the United States Constitution, laws such as those concerning libel, intellectual property, and pornography still determine how and if certain content can be published online.

In government

In February 2008, the *Bank Julius Baer vs. Wikileaks lawsuit* prompted the United States District Court for the Northern District of California to issue a permanent injunction against the website Wikileaks' domain name registrar. The result was that Wikileaks could not be accessed through its web address. This elicited accusations of censorship and resulted in the Electronic Frontier Foundation stepping up to defend Wikileaks. After a later hearing, the injunction was lifted.

On September 20th 2010 the Combating Online Infringement and Counterfeits Act was introduced, which if passed, would create two "Internet Blacklists" of Internet Domain Names, one that would be enforced by the Attorney General and the other would be optional. These blacklists would directly and purposefully censor the Internet in the United States. The bill was rejected however by Senator Ron Wyden (D-OR), this effectively killed off the bill until 2011 when it could be resubmitted to the committee.

In December 2010, both the offices of the White House Office of Management and Budget and the U.S. Air Force began blocking personnel from accessing more than 25 news organizations' websites on computers and mobile devices.

Block against Cuban websites

In March 2008, a New York Times story mentions that eNom is known to disable domain names which appear on a US Treasury Department blacklist. It describes eNom's disabling of a European travel agent's Web sites advertising travel to Cuba, which appeared on a U.S. Treasury Department list published by the Office of Foreign Assets Control (OFAC). The article's sources use words varying from "scandal" to "legally required" to describe "how Web sites owned by a British national operating via a Spanish travel agency can be affected by U.S. law", especially when the operation is as "mysterious" as that of the OFAC list.

By institutions

Institutions that provide Internet access for their members will sometimes censor this access in an attempt to ensure it is used only for the purposes of the institution. This includes censoring entertainment content in business and educational settings and censoring high-bandwidth services in settings where bandwidth is at a premium. Institutions may also block outside e-mail services. This is a precaution usually instigated out of concerns for network security.

Schools

Schools that accept funds from the E-rate program of LSTA grants for Internet connections are required by CIPA to have an "Internet safety policy and technology protection measures in place"

Many public schools have censorship programs built into their systems, but like most web blocking programs, they can't catch everything. Many schools default to using Internet filters to meet these requirements. However, the federal government leaves the local authorities to define what information needs to be censored, not each pupil's guardian. This arrangement has led many to question the censorship of Internet sites in the school system. At the same time these censoring programs can also block out a lot of useful information and limit students on what their research can get them. Some parents are also against many of the measures schools go to because they feel their children are being limited and their rights reduced. Some of the fears associated with Internet censorship in the school include: a predominant ideology, a specific view held by the filter manufacturer being imposed on the students, over blocking of useful information, under blocking of harmful information.

Libraries

Libraries also censor certain web pages, this may not be limited to pornography as it may extend to advertising sites, chat, gaming, social networking, and forums.

Individual websites

Some websites that allow user-contributed content practice censorship by banning users or pre-approving editorial contributions.

By content providers

Telecommunications companies

In 2007, Verizon attempted to block the abortion rights group Naral Pro-Choice America from using their text messaging services to speak to their supporters. Verizon claims it was in order to enforce a policy that doesn't allow their customers to use their service to communicate "controversial" or "unsavory" messages. Comcast, AT&T and many other ISP's have also been accused of regulating internet traffic and bandwidth.

By corporations abroad

Several US corporations including Google, Yahoo!, Microsoft, and MySpace practice greater levels of self-censorship in some international versions of their online services. This is most notably the case in these corporations' dealings in China.

Internet censorship in the United Kingdom

Internet censorship in the United Kingdom takes various forms, including blocking access to sites, and laws that criminalise publication or possession of certain material, particularly child pornography, within the United Kingdom.

Filtering

The Internet Watch Foundation (IWF) compiles and maintains a blacklist, mainly of child pornography URLs, from which 98% of commercial Internet customers in the UK are filtered. A staff of four police-trained analysts are responsible for this work, and the director of the service has claimed that the analysts are capable of adding an average of 65-80 new URLs to the list each week, and act on reports received from the public rather than pursuing investigative research.

British Telecommunications ISP passes Internet traffic through a service called Cleanfeed which uses data provided by the IWF to identify pages believed to contain indecent photographs of children. When such a page is found, the system creates a "URL not found" error page rather than deliver the actual page or a warning page. Other ISPs use different systems such as WebMinder.

Home Office Minister Vernon Coaker set a deadline of the end of 2007 for all ISPs to implement a “cleanfeed”-style network level content blocking platform. Currently, the only websites ISPs are expected to block access to are sites the Internet Watch Foundation has identified as containing images of child pornography. However such a platform is capable of blocking access to any website added to the list (at least, to the extent that the implementation is effective), making it a simple matter to change this policy in future. The Home Office has previously indicated that it has considered requiring ISPs to block access to articles on the web deemed to be “glorifying terrorism”, within the meaning of the new Terrorism Act 2006, saying "However, our legislation as drafted provides the flexibility to accommodate a change in Government policy should the need ever arise." The measures have been criticised for being inadequate as they only block accidental viewing and does not prevent content delivered through encrypted systems, file sharing, email and other systems.

In 2006, Home Office minister Alan Campbell pledged that all ISPs would block access to child abuse websites by the end of 2007. By the middle of 2006 the government reported that 90% of domestic broadband connections were either currently blocking or had plans to by the end of the year. The target for 100% coverage was set for the end of 2007, however in the middle of 2008 it stood at 95%. In February 2009, the Government said that it is looking at ways to cover the final 5%.

History

During 1996 the Metropolitan Police told the Internet Service Providers Association (ISPA) that the content carried by some of the newsgroups made available by them was illegal, that they considered the Internet Service Providers (ISPs) involved to be publishers of that material, and that they were therefore breaking the law. In August 1996, Chief Inspector Stephen French, of the Metropolitan Police Clubs & Vice Unit, sent an open letter to the ISPA, requesting that they ban access to a list of 132 newsgroups, many of which were deemed to contain pornographic images or explicit text.

This list is not exhaustive and we are looking to you to monitor your newsgroups identifying and taking necessary action against those others found to contain such material. As you will be aware the publication of obscene articles is an offence. This list is only the starting

point and we hope, with the co-operation and assistance of the industry and your trade organisations, to be moving quickly towards the eradication of this type of newsgroup from the Internet ... We are very anxious that all service providers should be taking positive action now, whether or not they are members of a trade association. We trust that with your co-operation and self regulation it will not be necessary for us to move to an enforcement policy.

—Chief Inspector Stephen French, quoted in *Web Control*

The list was arranged so that the first section consisted of unambiguously titled paedophile newsgroups, then continued with other kinds of groups which the police wanted to restrict access to, including *alt.binaries.pictures.erotica.cheerleaders* and *alt.binaries.pictures.erotic.centerfolds*.

Although this action had taken place without any prior debate in Parliament or elsewhere, the police, who appeared to be doing their best to create and not simply to enforce the law, were not acting entirely on their own initiative. Alan Travis, Home Affairs editor of the newspaper *The Guardian*, explained in his book "Bound and Gagged" that Ian Taylor, the Conservative Science and Industry Minister at the time, had underlined an explicit threat to ISPs that if they did not stop carrying the newsgroups in question, the police would act against any company that provided their users with "pornographic or violent material". Taylor went on to make it clear that there would be calls for legislation to regulate all aspects of the Internet unless service providers were seen to wholeheartedly "responsible self-regulation".

Demon Internet regarded the police request as "unacceptable censorship"; however, its attitude annoyed ISPA chairman Shez Hamill, who said:

We are being portrayed as a bunch of porn merchants. This is an image we need to change. Many of our members have already acted to take away the worst of the Internet. But Demon have taken every opportunity to stand alone in this regard. They do not like the concept of our organisation.
—*Observer*, 25 August 1996

Following this, a tabloid-style exposé of ISP Demon Internet appeared in the *Observer* newspaper, which alleged that Clive Feather (a director of Demon) "provides paedophiles with access to thousands of photographs of children being sexually abused".

During the summer and autumn of 1996 the UK police made it known that they were planning to raid an ISP with the aim of launching a test case regarding the publication of obscene material over the Internet. The direct result of the campaign of threats and pressure was the establishment of the Internet Watch Foundation (initially known as the Safety Net Foundation) in September 1996.

Internet Watch Foundation

Demon Internet was a driving force behind the IWF's creation, and one of its directors, Clive Feather, became the IWF's first chairman.

After 3 years of operation, the IWF was reviewed for the DTI and the Home Office by consultants KPMG and Denton Hall. Their report was delivered in October 1999 and resulted in a number of changes being made to the role and structure of the organisation, and it was relaunched in early 2000, endorsed by the government and the DTI, which played a "facilitating role in its creation", according to a DTI spokesman.

At the time, Patricia Hewitt, then Minister for E-Commerce, said: "The Internet Watch Foundation plays a vital role in combating criminal material on the Net." To counter accusations that the IWF was biased in favour of the ISPs, a new independent chairman was appointed, Roger Darlington, former head of research at the Communication Workers Union.

"Extreme" pornography

In 2003, after the murder of Jane Longhurst by Graham Coutts, a man who said he had an obsession with Internet pornography, the government announced plans to crack down on sites depicting rape, strangulation, torture and necrophilia. Liz Longhurst also campaigned to tighten laws regarding pornography on the Internet. In August 2005, the Government announced that instead of targeting production or publication, it planned to criminalise private possession of what the Government has termed "extreme pornography" Such adult pornography is illegal to possess as of January 2009.

In 2004 in Scotland, a committee of Members of the Scottish Parliament backed a call to ban adult pornography as the Equal Opportunities Committee supported a petition claiming links between porn and sexual crimes and violence against women and children. A spokeswoman said "While we have no plans to legislate we will, of course, continue to monitor the situation." In 2007, MSPs looked again at criminalising adult pornography, in response to a call from Scottish Women Against Pornography for pornography to be classified as a hate crime against women. This was opposed by Feminists Against Censorship.

In September 2008, Scotland announced its own plans to criminalise possession of what it termed "extreme" adult pornography, but extending the law further, including depictions of rape imagery.

"Girls (Scream) Aloud"

On 26 July 2007, UK tabloid newspaper *The Daily Star* reported that it had discovered an online text story about British pop group Girls Aloud that it described as "a chilling story detailing each singer's gory death in scenes that could be straight out of a horror movie", characterizing its author as "a vile internet psycho" and "a cyber-sicko". The news story said that *The Daily Star* had reported the content of the hosting website, "Kristen Archives" (a subsite of the ASSTR archive), to the IWF, and that the IWF had traced the site to the US. It also claimed that Interpol had been notified to help track down the site's operators and the writer of the story. An IWF spokesperson was reported as saying that since the site was hosted in the US, it fell outside the organization's remit, but that they were aware of the site. The spokesperson added that the site also contained "child abuse fantasy stories" and that they had passed on details of it to the British police.

Although the story, entitled "Girls (Scream) Aloud", had been published on a US website, British police carried out the investigation because the alleged author was identified as living in the UK. Although he had submitted the story under a pseudonym, he included

an email address which was reportedly traced. Officers from Scotland Yard's Obscene Publications Unit decided to take action over the story after consulting the Crown Prosecution Service (CPS), and on 25 September 2008 it was announced that the author, Darryn Walker, was to be prosecuted for the online publication of material that the police and the CPS believed was obscene. It was the first such prosecution for written material in nearly two decades, and was expected to have a significant impact on the future regulation of the Internet in the UK.

Walker appeared in court on 22 October 2008 to face charges of "publishing an obscene article contrary to Section 2(1) of the Obscene Publications Act 1959". He was granted unconditional bail, and his case was set for trial on 16 March 2009. However, at a directions hearing in January, the defendant made it known that given the seriousness of the case he would be represented by a QC (Queen's Counsel), following which the Crown Prosecution Service gave notice of its intention to similarly employ a QC, and the trial date was put back to 29 June 2009.

He appeared at Newcastle Crown Court on 29 June 2009 but the case was abandoned on what was supposed to be the first day of the trial, following the introduction of evidence from an IT expert. The CPS said that it had originally charged Walker as it believed that the story in question could be "easily accessed" by young fans of Girls Aloud. However, the IT expert showed that the article could only be located by those specifically searching for such material. A spokesperson for the CPS said that the prosecution was unable to provide sufficient evidence to contradict this new evidence and therefore took the decision that there was no longer a realistic prospect of conviction. Judge Esmond Faulks, presiding, returned a formal verdict of not guilty to the charge of "publishing an obscene article".

Introduction of Cleanfeed

Between 2004 and 2006, BT Group introduced its Cleanfeed technology which was then used by 80% of internet service providers. BT spokesman Jon Carter described Clean Feed's function as "to block access to illegal Web sites that are listed by the Internet Watch Foundation", and described it as essentially a server hosting a filter that checked requested URLs for Web sites on the IWF list, and returning an error message of "Web site not found" for positive matches.

2008 Internet regulation proposals

Culture, Media and Sport Select Committee Report

On 14 May 2008, in his oral evidence to the Culture, Media and Sport Select Committee's inquiry into harmful content on the Internet and in video games, Minister Vernon Coaker explained that the Prime Minister's Taskforce would be concerned not just with illegal content on the Internet, but also with "harmful and inappropriate content as well ... which may not be illegal but which cause all of us concern".

The Culture, Media and Sport Committee's report was published on 31 July 2008 and contained various recommendations among which were:

- That any approach to the protection of children from online dangers should be based on the probability of risk. We believe that incontrovertible evidence of harm is not necessarily required in order to justify a restriction of access to certain types of content in any medium.

- That the structure and funding of the Home Office Task Force on Child Internet Safety should be formalised.

- That terms and conditions which guide consumers on the types of content which are acceptable on a site should be prominent. It should be made more difficult for users to avoid seeing and reading the conditions of use: as a consequence, it would become more difficult for users to claim ignorance of terms and conditions if they upload inappropriate content.

- That the UK Council on Child Internet Safety should work with Internet-based industries to develop a consistent and transparent policy on take-down procedures with clear maximum times within which inappropriate material will be removed. This should be subject to independent verification and publication.

Culture Secretary

In June 2008 it was reported that Culture Secretary Andy Burnham had suggested the government should have a role in ensuring that content on the Internet met the same standards as that on television as "the boundaries between the two media blur". Burnham also raised the idea of warnings being applied to certain content on websites such as YouTube to help people "better navigate the internet". He referred to the Byron Review's March 2008 report, "Safer Children in a Digital World", saying that he thought people felt a "sense of risk and uncertainty about this world they are roaming". Burnham told journalists that he had an "open mind" about whether there was a need for a new Communications Act before the next General Election, indicating that his own preference was for smaller pieces of legislation as needed.

On 26 September 2008, Burnham delivered a keynote speech at the Royal Television Society conference in London, in which he said that the government planned to crack down on the internet to "even up" the regulatory imbalance with television, saying that "a fear of the internet" had caused a loss of confidence that had robbed the TV industry of "innovation, risk-taking and talent sourcing" in programming. He enlarged on his remarks in an interview published the following day in the *Daily Telegraph*, in which he said: "If you look back at the people who created the Internet they talked very deliberately about it being a space that governments couldn't reach. I think we are having to revisit that stuff seriously now ... There is content that should just not be available to be viewed. That is my view. Absolutely categorical." The article also suggested that Burnham was planning to negotiate with the Barack Obama administration "to draw up

new international rules for English language websites" and that another idea being considered was "giving film-style ratings to individual websites".

Burnham's words were criticized by technology journalist Bill Thompson, who pointed out that it was hard to reconcile his comments with the views of media regulator Ofcom that TV-style regulation of the Internet is both undesirable and unworkable, as the Internet is a network rather than a medium.

On 29 September 2008 Children's Secretary Ed Balls and Home Secretary Jacqui Smith announced the launch of the UK Council for Child Internet Safety (CCIS), which was supported by organisations including Google, Yahoo, BT, Microsoft, and Facebook, and which had an initial brief to deliver a "Child Internet Safety Strategy" to Prime Minister Gordon Brown in early 2009. The organisations were to work closely with government to deliver recommendations from Tanya Byron's March 2008 report, "Safer Children in a Digital World".

The group was also to look at ways of improving public awareness of child safety issues online, promote responsible online advertising to children and "provide specific measures to support vulnerable children and young people, such as taking down illegal internet sites that promote harmful behaviour." In addition they were also to investigate ways and means of "tackling problems around online bullying, safer search features, and violent video games." The CCIS was also to establish a voluntary code of practise for user-generated sites such as YouTube to agree a time limit for takedown of inappropriate content.

There have been concerns over the increasing amount of Internet regulation and fears that the Internet may become even more restricted in future.

Libel laws

In a 27 December 2008 newspaper interview, UK Culture Minister Andy Burnham said that the Government was considering changing the UK's libel laws to give people access to cheap low-cost legal recourse if they were defamed online. He said that the legal proposals were being drawn up by the Ministry of Justice.

Chapter 13

Internet Censorship in Thailand and Pakistan

Internet censorship in Thailand

Internet censorship is effected in Thailand by two methods. The Royal Thai Police blocks approximately 32 500 websites and the Communications Authority of Thailand a further unspecified number directly at Thailand's Internet gateway.

Informal requests

The Ministry of Information and Communication Technology (MICT) , blocks indirectly by informally “requesting” the blocking of websites by Thailand's 54 commercial and non-profit Internet Service Providers (ISPs). Although ISPs are not legally required to accede to these “requests”, MICT Permanent Secretary Kraisorn Pornsuthee has written in 2006 that ISPs who fail to comply will be punitively sanctioned by government in the form of bandwidth restriction or even loss of operating license. This is a powerful compulsion to comply.

Coups

On September 19, 2006, the Thai military staged a bloodless coup d'état against the government of elected Prime Minister Thaksin Shinawatra. The fifth official order signed by coup leader General Sonthi Boonyaratglin on September 20, the first day following the coup, was to enforce Web censorship and appointing Dr. Sitthichai Pokaiudom “The Official Censor of the Military Coup” as Minister of ICT.

History

Prior to the military coup d'état, in September 2006, 34,411 Internet web sites were blocked. The top cited reasons are: Pornography 56%, sale of sex equipment 13%, and threats to national security 11%, which includes criticisms of the king, government or military. This figure represents blocking done by all three government agencies.

In October 2006, MICT blocked 2475 websites by "request"; by January 11, 2007, this number had risen to 13,435 websites, a jump of more than 500%. This brings the current total of websites blocked to more than 45,000. All websites are blocked in secret and the criteria for censorship has never been made public by government. However, the MICT blocklist must be made available to ISPs to block.

Although the great majority of censored sites are pornographic, the list is liberally salted with an attempt to block all anonymous proxy servers which serve to circumvent Web-blocking and Internet gambling sites. Pornography and gambling are specifically illegal in Thailand.

Methods

Websites are blocked by Uniform Resource Locator (URL) and/or IP address. However, only about 20% of blocked sites are identified by IP; the remaining 80% are unable to be identified at a physical location. If these sites could be identified as being located in Thailand, legal action could be taken against their operators. Thus, lack of IP is a major oversight.

Several technologies are employed to censor the Internet such as caching, blacklisting domain name or IP address, or simply redirection to a government homepage. Blacklisting the website is beneficial for this kind of web censorship as the webmasters would be unaware that their websites are being blocked. This measure is said to be used to make unpleasant websites appear unavailable.

Many censored web sites previously redirected the user to a site hosted by the Ministry of Information and Communication Technology (MICT) which states that the requested destination could not be displayed due to improper content. It should also be noted that censorship of the Internet in Thailand is currently for website access only. Unlike China's “Great Firewall”, which censors all Internet traffic including chat conversation via Instant Messaging, Thai Internet users are still able to interact with other users without being censored. However, current policy is to use a system of transparent proxies so that the user receives system, server, TCP and browser error messages when trying to access blocked sites leading the user to believe that the failure is caused in the Internet itself.

Search engine giants, Google and Yahoo!, were approached to investigate the potential capability for blocking access to their cached web pages in Thailand, a common technique used to circumvent blocking. The search engines were also asked about blocking by keyword search which is used effectively in China to censor the Internet. Google, at least, has made public a statement that it has no intention of blocking any sites to users in Thailand.

Wayback Machine, a project of Archive.org, currently caches 85 billion inactive web pages. Some of these are now being blocked by the MICT. With 100 million active web pages, 10% of which are thought to be pornographic, the effect of MICT's censorship will only be negligible.

Another, more disturbing, trend is the censorship of anti-coup websites such as 19 September Network against Coup d'Etat, which has been blocked six times, as of Febreuary 2007, with government refusing to acknowledge responsibility for the blocking.

Internet webboards and discussion forums such as Midnight University, Prachatai.com and Pantip.com have all been blocked so reasonable political discussion has been rendered impossible. Prachatai and Pantip have chosen to self-censor, closely monitoring each discussion, in order to remain unblocked. In addition, video sharing sites such as Camfrog have recently been blocked with the grounds given that people were "behaving indecently" on webcams; the block was later reversed when it was discovered that Camfrog provided a principal means of communication for the handicapped, elderly and shut-ins. Other video sharing sites such as Metacafe remain blocked however. The entire video upload website, YouTube, has suffered several blockings, including a complete ban between April 4, 2007 and August 31, 2007 due to a video which was considered to be offensive to the monarchy; YouTube's parent company, Google, was reported in the press to have agreed to assist the MICT in blocking individual videos rather than the entire website. The entire YouTube site block persisted for nearly five months, despite the fact that the video challenged by the MICT was voluntary deleted by the user who posted it.

Southern insurgency

Most sites concerning the violent political situation in Thailand's Muslim South are blocked, specifically those in support of the Patani United Liberation Organisation (PULO), a banned group which works for a separate Muslim state, including PULO's appeals to the United Nations for redress.

External news sites

In addition, some web pages from BBC One, BBC Two, CNN, Yahoo! News, Seattle (USA) *Post-Intelligencer* newspaper, and *The Age* (Melbourne, Australia) newspaper dealing with Thai political content are blocked. More recently, all international coverage of Thaksin-in-exile has been blocked, including interviews with the deposed PM.

Thailand blocked Google's video sharing site YouTube beginning on April 4, 2007, but Reuters reported on 6 April 2007 that the search company promised to help the Thai government block certain material on the site, making the rest legal to display in Thailand. The block remained in place until August 4, 2007.

Although the “interpretive biography” of Thailand's King Bhumibhol Adulyadej, *The King Never Smiles* by Paul Handley (Yale University Press) was published in July 2006, websites concerning the book had been blocked as far back as November 2005. As no advance reading copies or excerpts were made available, these sites were censored based on the book's title alone. All sites with links to sales of the book are still blocked, including Yale University Press, Amazon. com, Amazon UK and many others.

Protests

Interference in communication, including the Internet, was specifically prohibited by Section 37 of the 1997 “People's” Constitution and free speech protected by Section 39. However, following the pattern of past coups, the military's first action was to scrap the Constitution and establish drafting a new one. Nevertheless, the MICT has commissioned the Law Faculty of Sukhothai Thammathirat Open University to find laws or loopholes which permit such censorship, and several other organizations have filed petitions with Thailand's National Human Rights Commission (NHRC).

Midnight University

Midnight University has filed petitions simultaneously with the NHRC and Thailand's Administrative Court. As the Court and the Council of State can find no laws which permit Internet censorship, Midnight University has been granted a restraining order against further blocking, pending resolution of its legal case. This makes Midnight University the only legally-protected website in Thailand.

FACT

Freedom Against Censorship Thailand (FACT) filed a petition against censorship before the NHRC on November 15, 2006. FACT's petition is still open for signatures and is actively seeking international support. Though NHRC has no enforcement capability and is therefore rarely able to extract evidence from government bodies, the MICT agreed to cooperate with the NHRC on January 26, 2007.

On February 9, 2007, FACT filed an official information request with the MICT under the Official Information Act of 1997. The request contains 20 questions and is signed by 257 individuals supported by 57 international civil liberties and human rights groups. The MICT refused to reply citing grounds of “national security” and “interference with law enforcement”; its secret blocklist, criteria used for censorship and specific procedures it uses remain private. On March 23, 2007, FACT filed a complaint requiring an investigation within 60 days by the Official Information Commission under the Prime Minister's Office. FACT stated that, should the complaint fail, it would seek a restraining order against further censorship through Thailand's legal system.

Software

Software applications for circumventing web-blocking are readily available. Tor is in used through software including XeroBank Browser (formerly Torpark) and Vidalia, and a number of other proxied solutions including Proxify, Six-Four, phproxy are also used. Freenet is another popular solution. Available for free download from the Internet, these packages are also published on disk by FACT. The Information and Communications Technology (ICT) Minister has said in an interview in the Bangkok Post that he has not blocked these methods because "using proxies to access illegal sites are illegal, whereas using proxies to access legal sites is legal."

Blocking websites containing lese majeste content

ICT Minister Mun Patanotai announced on October 29, 2008, plans to introduce an internet gateway system costing up to 500 million baht to block sites considered to promote lese majeste materials. The Minister said the system could also be used to block other websites considered inappropriate, such as those of terrorist groups or selling pornography, but the ministry will focus first on websites with content deemed insulting to the Thai monarchy. The Criminal Code states that whoever defames, insults or threatens the King, Queen, the heir-apparent or the Regent, shall be jailed for three to 15 years, but the statute is broadly interpreted to apply to any mention of the institution of royalty that is less than flattering.

Internet censorship in Pakistan

The **internet censorship in Pakistan** is done by the government of Pakistan by means of routing all connections through a central exchange which is administered by the Pakistan Internet Exchange. Pakistani ISPs are also under orders to block certain websites on their own routers. A common victim by major ISPs in Pakistan was the weblogs hosted at blogspot.com (The blanket ban on the blogspot.com blogs is lifted), amongst other important social networking websites.

History and law

The Government of Pakistan some years back established the Pakistan Internet Exchange (PIE), as a means to monitor all incoming and outgoing Internet traffic from Pakistan. The primary purpose of PIE is to filter content as the government deems fit. A secondary purpose is to keep track of all incoming and outgoing e-mail, which by parliamentary order are kept for a period of at least three months.

The Pakistan Telecommunication Company Ltd (PTCL) announced in April, 2003 that it would be stepping up monitoring of pornographic websites. "Anti-Islamic" and "blasphemous" sites were also monitored. In early March 2004, the Federal Investigation Agency (FIA) ordered Internet service providers (ISPs) to monitor access to all pornographic content. The ISPs, however, displayed absence of technical know-how, and advocated that the PTCL would be better fit to carry out FIA's requirement. A Malaysian firm was then hired to provide a filtering system but was a failure.

YouTube

YouTube was blocked in Pakistan following a decision taken by the Pakistan Telecommunication Authority on February 22, 2007 because of the number of "non-Islamic objectionable videos." One report specifically names Fitna, a controversial Dutch

film, as the basis for the block. Pakistan, an Islamic republic, has ordered its ISPs to block access to YouTube "for containing blasphemous web content/movies."(Blasphemy law in Pakistan calls for life imprisonment or death.) The action effectively blocked YouTube access worldwide for several hours on February 24.

This follows increasing unrest in Pakistan over the re-printing of the Jyllands-Posten Muhammad cartoons which depict satirical Criticism of Islam. However, it has been suggested by some Pakistani vigilante web sites and electoral process watchdog groups that the block was imposed largely to distract viewers from videos alleging vote-rigging by the ruling MQM party in the recently concluded general elections. Allegations of suppressing vote-rigging videos by the Musharraf administration are also being leveled by Pakistani bloggers, newspapers, media, and Pakistani anti-Musharraf opposition parties. The ban was lifted on February 26, 2008.

Supreme Court directive

The Supreme Court on March 1, 2006 directed the government to keep tabs on Internet sites displaying the Prophet Muhammad cartoons and called for an explanation from authorities as to why these sites had not been blocked earlier. A three-member bench headed by Chief Justice Iftikhar Muhammad Chaudhry, summoned the country's Attorney General as well as senior communication ministry officials on March 13 to give a report of "concrete measures for implementation of the court's order". , On March 2, 2006, in pursuant to a Petition filed by Dr. Mohammed Imram Uppal under Article 184(3) of the Constitution of Pakistan, the Supreme Court sitting *en banc* ordered the Pakistan Telecommunications Authority (PTA) and other government departments to adopt measures for blocking websites showing blasphemous content. The Court also ordered Attorney General Makhdoom Ali Khan to explore laws which would enable blocking objectionable websites. In announcing his decision, Chief Justice Iftikhar Muhammad Chaudhry, said, "We will not accept any excuse or technical objection on this issue because it relates to the sentiments of the entire Muslim world. All authorities concerned will have to appear in the Court on the next hearing with reports of concrete measures taken to implement our order," which was scheduled on March 13, 2006.

Consequently, the government kept tabs on a number of websites hosting the cartoons deemed to be sacrilegious. This ban included all the weblogs hosted at the popular blogging service blogger.com, as some bloggers had put up copies of the cartoons – particularly many non-Pakistani blogs.

On the hearing on March 14, 2006, the PTA informed the Supreme Court that all websites displaying the Muhammad cartoons have been blocked. The bench issued directions to Attorney General of Pakistan Makhdoom Ali Khan to assist the court on Monday on how it could exercise jurisdiction to prevent the availability of blasphemous material on websites the world over.

The blanket ban on the blogspot.com blogs was lifted on May 2, 2006 n:Blogspot ban lifted in Pakistan. Shortly thereafter the blanket ban was reimposed, and extended to Typepad blogs. The blanket ban on the blogspot.com blogs is lifted again.

Highcourt Karachi directives

The High Court of Sindh Karachi on sept 29- 2010 has directed the Pakistan Tele Communication Authority to take steps to Block all dirty wesites on internet in paksiatn, such orders were Solicited in CONSTITUTIONAL PETION No-1288/2010 filed By advocate FAYAZ SAMOR for registration of case of cyber stalking of a victum student girl, the councel placed the report of FOX-NEWS showing pakistan no-01 visitor of sexy web-sites

Other blocked websites

Pakistan also allegedly blocked websites promoting ethno-separatism.

On May 19-20 2010, Pakistan's Telecommunication Authority (PTA) imposed a ban on, YouTube, Flickr and Facebook in response to a competition entitled 'Draw Muhammad Day" on Facebook. The competition involved drawing caricatures and cartoons depicting the image of the Prophet of Islam, Muhammad. It is to be noted that the ban imposed on Facebook was as per court ruling (the Lahore High Court) while the ban on the other websites was imposed arbitrarily by the PTA on the grounds of 'objectionable content' on these websites. It is also notable that the Facebook Terms Of Service were clearly being violated by the said page, and Facebook did not remove the page of its own accord. It had responded previously to such requests by the Pakistani government by doing as it asked, as was the case of Facebook pages being created to promote peaceful demonstrations in Pakistani cities and being banned because of 'inciting violence'.

How the Internet is monitored

The government of Pakistan has a simplistic IP based filtering procedure in place, for example since all websites hosted on blogspot resolve to the same IP address, they were blocked. However since the PIE uses Cisco routers to block traffic, which are capable of more complex filtering rules, the government removed this blanket block on all blogspot weblogs few months ago, now it has the capability to only target specific websites.

As all Internet traffic is routed through the PIE, Pakistani ISPs have also been ordered to also block certain websites on their routers. Previously, all the major ISPs in Pakistan blocked weblogs hosted at blogspot.com, But now its been unblocked.