

**Refugee Review Tribunal  
AUSTRALIA**

**RRT RESEARCH RESPONSE**

**Research Response Number:** IRN33389  
**Country:** Iran  
**Date:** 29 May 2008

Keywords: Iran – Internet censorship

This response was prepared by the Research & Information Services Section of the Refugee Review Tribunal (RRT) after researching publicly accessible information currently available to the RRT within time constraints. This response is not, and does not purport to be, conclusive as to the merit of any particular claim to refugee status or asylum. This research response may not, under any circumstance, be cited in a decision or any other document. Anyone wishing to use this information may only cite the primary source material contained herein.

---

**Questions**

**1. If a website that is based in Iran is accessible from Australia is it possible that in Iran it would be not accessible or frozen to all users in Iran?**

**RESPONSE**

**1. If a website that is based in Iran is accessible from Australia is it possible that in Iran it would be not accessible or frozen to all users in Iran?**

According to a study conducted by the OpenNet Initiative the Iranian authorities are known to sometimes allow an offending Iranian website to remain online while limiting access to the website for Internet users in Iran. Such censorship is enabled by the filtering software which Iranian Internet service providers (ISPs) are required to run. According to the study: “prosecutors can bring charges to close, suspend, or filter sites that the [Supreme Council of the Cultural Revolution established monitoring] committee has not itself closed, and authorities do pressure ISPs to block sites which the committee has not deemed worth action (including sites associated with legal, reformist political parties)”. The study relates that: “ParsOnline, a major ISP, filters several blogging sites that the committee has not ordered blocked”. The study also found of Iran’s various filtering activities that: “testing showed that online content in the Farsi language is more likely to be blocked than is comparable content in the English language”. The OpenNet Initiative’s study of Internet filtering in Iran was conducted over 2004-2005. Relevant extracts from the OpenNet Initiative study follow below. The OpenNet Initiative is a multi-partner investigation of Internet censorship established by “Citizen Lab at the Munk Centre for International Studies, the University of Toronto, Berkman Center for Internet & Society at Harvard Law School, the Advanced Network Research Group at the Cambridge Security Programme, University of Cambridge, and the Oxford Internet Institute, Oxford University”.

Our testing showed that online content in the Farsi language is more likely to be blocked than is comparable content in the English language. We found 499 sites blocked out of 1477 tested (34%) in our November round of tests, and 623 sites of 2025 tested (31%) filtered in our December round. The Iranian state has effectively blocked access of its citizens to many pornographic online sites, most anonymizer tools (which allow users to surf the Internet without detection), a large number of sites with gay and lesbian content, some politically sensitive sites, women's rights sites, and certain targeted Web logs ("blogs"), among other types of sites.

Iran's filtering regime is backed up by an extensive series of laws that control the publication of sensitive information. The press is restrained through a broad set of media-related laws, especially the Press Law of 1986, which includes licensing and substantive regulations. Individuals who subscribe to Internet service providers (ISPs) must promise in writing not to access "non-Islamic" sites. The law requires ISPs to install filtering mechanisms that cover access to both Web sites and e-mail. Punishment for violations of content-related laws can be harsh.

...Iran has comparatively high freedom of access to the Internet, pricing notwithstanding. Some observers suggest that regulation may increase as conservative officials increase their control in the state and begin to realize the power of the Internet medium. Private ISPs must be approved by both DCI and the Ministry of Culture and Islamic Guidance. ISPs must implement filtering mechanisms for Web sites and e-mail. In 2001, TCI issued regulations requiring ISPs that obtain access from it to filter all materials presumed immoral or contrary to state security, including the Web sites of opposition groups. While TCI's rules have not been routinely enforced, ISPs could face legal action if they do not comply with government-mandated filtering lists, and more than ten ISPs have been shut down for not installing filters.

...Internet content regulation in Iran evolves and changes rapidly. The Iranian state has exerted strong control over traditional media since its inception. As the Internet has grown in popularity as a venue for anti-government or anti-Islamic activity, the state has moved to increase its controls over Internet material by filtering sites from outside Iran and regulating the activities of sites and online journalists that operate from within Iran. Most regulations focus on restricting access to foreign sites and regulating domestic sites, and not on controlling users' behavior.

Internet content regulation in Iran occurs at multiple levels, through multiple methods. ISPs filter foreign sites using Secure Computing's SmartFilter software, which is developed in the United States. Sites based in Iran can be shut down, suspended, or filtered through direct methods (state orders or pressure) or indirect methods (informal pressure on ISPs); authors and technical staff of sites have been questioned and even arrested. Activists have expressed concern that recent government activities and proposed laws indicate an expansion of censorship of both domestic and foreign Internet sites.

While Iran does not have Internet-specific regulations for content, the state imposes strong controls on Internet materials under the country's Press Law. For example, in May 2004, the Prosecutor-General stated that authors of material posted on Web sites created in Iran risked prosecution if they did not respect the national constitution and the Press Law. When sites within Iran are shut down, their owners can appeal to the judiciary on the grounds that they were inappropriately closed or suspended; site owners occasionally win these appeals.

...Iran's controls on Internet content have increased recently. In the campaign for the February 2004 parliamentary elections, Internet filtering (as well as controls over traditional media) increased noticeably. In mid-2004, the Supreme Council of the Cultural Revolution established a committee to monitor Iranian-based sites for closure; the Council focuses particularly on pornographic or politically sensitive sites. However, prosecutors can bring

charges to close, suspend, or filter sites that the committee has not itself closed, and authorities do pressure ISPs to block sites which the committee has not deemed worth action (including sites associated with legal, reformist political parties). Technology officials have expressed concern that some filtering was ordered by the Chief Prosecutor of Tehran outside proper legal channels, which consists of the five-man committee under the Supreme Council (of which the Chief Prosecutor is only one member). ParsOnline, a major ISP, filters several blogging sites that the committee has not ordered blocked. State officials detained IT staff from several reformist Web sites to force them to turn over passwords to the hosting accounts for those sites. The sites were apparently shut down.

Arrests and detentions of bloggers and online journalists have increased in recent years. More than 20 people have been arrested and charged in connection with news Web sites (including bloggers, journalists, and technical staff) since the summer of 2004. Some online journalists who were released in December 2004 appeared on television to confess to committing crimes, but later accused the state of holding them in solitary confinement and subjecting them to torture. Even after being released, many of these journalists continued to face pressure and threats from authorities. In addition, recent reports indicate that various agencies within Iran have tried to register every Internet site based in Iran. Some major blogging sites, including Blogger and Persianblog, have reportedly been filtered.

Iran may be moving to augment further its Internet controls. The New York Times reports that the Iranian judiciary is drafting a law that will define cybercrimes and authorize punishment for “anyone who disseminates information aimed at disturbing the public mind through computer systems.” The proposed law would ban criticizing the state and its officials, buying and selling alcohol, connecting to sex sites, and distorting the words of the “Supreme Guide.” Drafts of the bill prohibit activity that “poses a threat for the country’s internal or external security”; punishments include fines and prison sentences of up to 15 years if the information is passed to foreign states or organizations. The law makes ISPs, ICPs, hosting companies, and cybercafe owners responsible for monitoring all content to which they offer access and authorizes cancellations of permits or temporary closure of violators (previous versions authorized jail time for executives of companies). This bill was sent to the head of Iran’s Judiciary Office in late November 2004.

Filtering is an important component of Iran’s content controls. In January 2003, the state created a commission to compile lists of sites (“blacklists”) to block. In May 2003, Iran announced plans to block 15,000 sites by providing a blacklist to ISPs. At the time, ministers were quoted as saying they wanted to “block access to immoral sites as well as political sites which rudely make fun of religious and political figures in the country (‘Internet Filtering in Iran in 2004-2005: A Country Study’, 2005, OpenNet Initiative website, 1 April [http://opennet.net/sites/opennet.net/files/ONI\\_Country\\_Study\\_Iran.pdf](http://opennet.net/sites/opennet.net/files/ONI_Country_Study_Iran.pdf) – Accessed 29 May 2008 – Attachment 1; for information on the OpenNet Initiative project, see: ‘About ONI’ (undated), OpenNet Initiative website <http://opennet.net/about> – Accessed 29 May 2008 – Attachment 3).

A December 2007 study of Internet censorship in Iran by Dr Nima Mina provides further background on Internet censorship in Iran. The final paragraph notes details of the manner in which Iranian bloggers have, since mid-2007, been “ordered to register their blogs through a virtual government office” or risk being “filtered and blocked for readers in and perhaps outside of the country”. It may be of interest that the report discusses an example of Internet censorship in Iran in which Iranian Internet users were prevented from accessing an Iranian website which began posting material critical of the Iranian government: “In February 2007, as well as earlier during 2006, the website Baztab [www.baztab.ir] was temporarily blocked for readers inside Iran”. Details of the episode are covered in the penultimate paragraph of the extracts presented below. Mina’s 2007 study was produced for the US and German

government funded George C. Marshall European Center for Security Studies. Some pertinent extracts follow:

According to official figures published by the Iranian Ministry of Communication and Information Technology, the total number of internet users in 2001 was estimated at 1 million. This number increased to 5 million in 2005, 11 million in 2007 and by 2009, 25 million users are expected. At present, there are 650 Internet Service Providers (ISPs) and 150 Internet Content Providers (ICPs) active in Iran. A company named Data Corporation is currently the biggest ISP in Iran and the main link to the state telecommunications authority. Most other ISPs receive their access to the internet through Data Corporation and are subject to restrictions imposed upon them by the government through this company.

Since the internet and related technologies have come to the Islamic Republic, the government has issued preliminary regulations for the activity of ISPs. According to these regulations, all private ISPs must be in possession of filtering facilities to block specific websites included in the government's "black lists," which contain millions of addresses. Since mid-2006, the leadership of the Islamic Republic seems to have centralized the filtering practice in order to selectively block certain websites. The government's "black lists" are compiled and updated by the Supreme Council for Communication Affairs. The Committee for the Determination of the Applicability of Filtering, composed of three members representing the state radio and television organization, the Ministry of Intelligence and Security (MOIS)<sup>57</sup> and the Supreme Council of Cultural Revolution is the country's central executive organ steering internet filtering policies. Interestingly, the Ministry of Communication and Information Technology has no representative in this committee.

The centralization process seems to be constantly undermined on all levels by the Islamic Republic's own government organs. From time to time, the Judiciary, which is not represented in the "filtering committee" either, gets involved directly and issues instructions and prohibitions to ISPs. Likewise, the filtering committee's policies seem to be enforced with various degrees of strictness in different parts of the country. In the southern and south-eastern border regions, which were destabilized by ethnic and religious conflicts during the past years, filtering and blocking of unapproved websites is enforced more strictly. Occasionally, the internet connection of entire provinces has been switched off. On the other hand, users can often access blocked websites during the night or from specific locations like university computer centers and newspaper editorial offices.

So far, the "filtering committee" has never justified its decisions to block certain internet sites. The only explicitly formulated filtering rule is rather vague and was issued by the Supreme Council for Cultural Revolution. It requires the ban of "heretic publications that contradict the principles of Islam and insult its holiness and advertise for forbidden political groups and parties."

In mid-July 2005, a bill about "computer crimes" was agreed upon and sent on to the 7th parliament of the Islamic Republic for approval by the newly constituted cabinet of Mahmoud Ahmadinejad. The bill claimed to target "economic crimes" committed with computers as well as pornography and hacker activities, but in reality it was solely applied to "political offenses." At about this time, the popular websites Flickr, YouTube, Wikipedia and the New York Times were banned and the maximum speed of broadband internet connections was limited by law to 128 kilobytes per second (KBps), in order to prevent uploads and reports of large audio and video files over the internet.

...Internet filtering, website blocking and even the surveillance of the mobile telephone network are not just weapons against oppositional activity outside the regime. Occasionally they are also used as instruments in the power struggle between rival factions in the conservative camp in the leadership of the Islamic Republic. In February 2007, as well as

earlier during 2006, the website Baztab [www.baztab.ir] was temporarily blocked for readers inside Iran. The license owner and general editor of Baztab is Mohsen Rezai, a member of the Islamic Republic's Expediency Council and a veteran of the security and intelligence network since the early 1980s, notably the Islamic Revolutionary Guard Corps (IRGC) and the MOIS. Baztab was blocked because it published articles that criticized the work of the nuclear negotiation team of the Islamic Republic, at that time lead by the cleric Hassan Rohani.

...On 5 January 2007, the prosecutor Said Mortazavi ordered all Iranian ISPs to block a number of blog service providers. Later, in June, all Iranian bloggers were ordered to register their blogs through a virtual government office. In the registration process, bloggers who write under a pseudonym have to disclose their real identity and all access data for their blogs. Individuals who do not comply with these orders must expect their blogs to be filtered and blocked for readers in and perhaps outside of the country. The government can indeed order Iran-based services like www.persian.com to filter unregistered blogs. At present, there are 780,000 blogs registered with PersianBlog, 10 % of which are updated daily. The judiciary's registration directive triggered a wide civil resistance action by non-conformist bloggers. Even some bloggers who publish under their own names and live inside the country participated in the resistance. The journalist and women's movement activist, Parastoo Dokouhaki, for example, published a banner in her blog announcing that she would boycott the registration (Mina, N. 2007, 'Blogs, Cyber-Literature and Virtual Culture in Iran', George C. Marshall European Center for Security Studies website, Occasional Paper Series, no.15, December [http://www.marshallcenter.org/site-graphic/lang-en/page-pubs-index-1/static/xdocs/research/static/occpapers/occ-paper\\_15-en.pdf](http://www.marshallcenter.org/site-graphic/lang-en/page-pubs-index-1/static/xdocs/research/static/occpapers/occ-paper_15-en.pdf) – Accessed 29 May 2008 – Attachment 2).

## List of Sources Consulted

### Internet Sources:

Google Search engine <http://www.google.com.au>

## List of Attachments

1. 'Internet Filtering in Iran in 2004-2005: A Country Study', 2005, OpenNet Initiative website, 1 April [http://opennet.net/sites/opennet.net/files/ONI\\_Country\\_Study\\_Iran.pdf](http://opennet.net/sites/opennet.net/files/ONI_Country_Study_Iran.pdf) – Accessed 29 May 2008.
2. Mina, N. 2007, 'Blogs, Cyber-Literature and Virtual Culture in Iran', George C. Marshall European Center for Security Studies website, Occasional Paper Series, no.15, December [http://www.marshallcenter.org/site-graphic/lang-en/page-pubs-index-1/static/xdocs/research/static/occpapers/occ-paper\\_15-en.pdf](http://www.marshallcenter.org/site-graphic/lang-en/page-pubs-index-1/static/xdocs/research/static/occpapers/occ-paper_15-en.pdf) – Accessed 29 May 2008.
3. 'About ONI' (undated), OpenNet Initiative website <http://opennet.net/about> – Accessed 29 May 2008.