Questions
1. Please provide brief general information on the situation for Internet Service Providers in Iran.

RESPONSE

1. Please provide brief general information on the situation for Internet Service Providers in Iran.

A March 2008 report on internet freedom from the NGO Reporters Without Borders classifies the Iranian authorities as an “internet enemy”:

The main access providers are dependent on the Iranian Telecommunications Network (TCI) which is a state-run business. Despite the presence of private companies, the state remains the main player in the market.

The number of Internet-users has increased markedly. There were only just over one million in 2004 but now there are about 18 times more of them. According to figures published by the official news agency, ISNA, privately-owned access providers have opened more than 400,000 points of access and the government 112,000. More than 4,000 schools are also connected. In this way, the Internet has become a precious tool for activists, who can send their messages throughout the country. In a bid to curb criticism of the government, the Culture and Islamic Orientation Minister, Mohammed Saffar Harandi, insisted on 17 February 2008, on the fact that websites not registered with the ministry would be closed.
Control stepped up

The authorities have banned high speed connections since 2006, a measure which could be explained by a concern not to overload the Iranian network, which is of very poor quality, but it could also be interpreted as a desire to block western cultural products – films and songs – reportable on the Net. The Council of Ministers has defined the criteria under which a website could be considered “illegal”: publications insulting Islam or monotheist religions, those which disseminate separatist ideologies, those publishing false news or damaging private life.

The government on 27 November 2006 established regulations under which website managers were ordered to register with the authorities and created an “Internet surveillance body” directly reporting to the Ministry for Culture and Islamic Orientation, responsible for combating the publication of “false news”. As a result the website of the conservative newspaper Baztab.com which is close to the former commander of the Revolutionary Guards, Mohsen Rezai, and highly critical of President Mahmoud Ahmadinejad, has been regularly subjected to legal proceedings for publishing “false” news, “in breach of the Constitution”, “damaging private life” or “the unity of the country”. It was banned by the Council of State on 29 March 2007 and its offices were closed on the orders of the authorities, in September, in the first application of the November 2006 regulations. A judge also ordered censorship of the website of the independent agency ILNA, founded in 2003 and close to the reformists (‘Internet Enemies – Iran’ 2008, Reporters Without Borders, 13 March http://www.rsf.org/imprimer.php3?id_article=26154 – Accessed 13 May 2009 – Attachment 1).

A November 2005 Human Rights Watch report on internet freedom in Iran, produced as part of a publication titled False Freedom: Online Censorship in the Middle East and North Africa, states that: “In July 2005, Iran was home to 683 Internet Service Providers (ISPs)”. This report also provides a thorough list of the regulations to which Iranian ISPs must adhere, and a list of outlawed online activities. It may be of interest to note that this report claims that, in a 2004 crackdown on internet freedom in Iran, “[t]he authorities detained contributing journalists and technical staff rather than high-profile political leaders under whose names these Web sites operate”:

Iranian Web sites – despite a desperate effort on the part of the government to control the Internet – nevertheless continue to express opinions that the country’s print media would never run. The government has imprisoned online journalists, bloggers, and technical support staff. It has blocked thousands of Web sites, including – contrary to its claims that it welcomes criticism – sites that criticise government policies or report stories the government does not wish to see published. It has sought to limit the spread of blogs by blocking popular Web sites that offer free publishing tools for blogs.

…Internet use is soaring in Iran. In 2001, an estimated 250,000 Iranians were online. By July 2005, that number had climbed to 6.2 million. The Telecommunication Company of Iran (TCI), a private company the government established to implement the Ministry of Communications and Technology’s policies, estimates that 25 million Iranians will be online by 2009. In July 2005, Iran was home to 683 Internet Service Providers (ISPs). The Data Communication Company of Iran (DCCI), a subsidiary of the TCI, is the nation’s most widely used ISP.

…When asked what regulations specifically govern the Internet in Iran, the Iranian government referred Human Rights Watch to a Data Communication Company of Iran (DCCI) Web page. According to these regulations, promulgated by the Supreme Council for Cultural Revolution, access service providers (ASPs) “are required to provide filtering
systems to prevent access to prohibited immoral and political sites” and to “prevent indirect access through proxy servers.”

The council’s regulations also stipulate that officers of ISPs must be Iranian nationals with an allegiance to the Constitution of the Islamic Republic; a member of a faith recognized by the constitution; possess technical skills with the minimum required academic degree and be at least 25 years old; not have immoral reputation or a criminal conviction; not belong to an anti-revolutionary organization or support one (those who have been convicted of acting against internal or external security or are known to be acting against the Islamic Republic cannot be officers of ISPs).

ISPs are further “legally liable and bound by the following rules and commitments:”

5.3.1. ISPs and their subscribers are responsible for the content they distribute on the network.

Note: 5.3.1. does not apply to providing access to news/information sources. […]

5.3.3. ISPs must implement filtering devices. Filtering standards will be provided by the Council. […]

5.3.5. ISPs are required to record all user information and IP addresses and provide this information to the Ministry of Post and Telegraph. […]

5.3.14. ISPs can only access the Internet through authorized ASPs.

Regulations targeting ISPs, such as rule 5.3.1, impose a heavy and perhaps technically impossible burden on the data carrier, one that is incompatible with protecting the right to freedom of expression online. Such regulations run counter to the principle of free expression online by imposing a regulatory burden on ISPs that—to the extent that it is even feasible given the nature of data flow online—forces them into the role of censors.

Rule 5.3.5 requires ISPs “to record all user information and IP addresses and provide this information to the Ministry of Post and Telegraph.” Such a disclosure requirement constitutes by its sweeping nature a violation of the right to seek, receive, and impart ideas anonymously.

The Council then enumerates what online activities are prohibited:

6. Production and dissemination of the following by ISPs and their subscribers is prohibited:

   6.1. Publishing anti-Islamic material
   6.2. Insulting Islam.
   6.3. Publishing material that is against the Constitution or which affects the independence of the nation.
   6.4. Insulting the leader.
   6.5. Insulting religious sanctities, Islamic decrees, values of the Islamic revolution or political ideologies of Imam Khomeini.
   6.6. Material that will agitate national unity and harmony.
   6.7. Causing public pessimism about the legitimacy and efficacy of the Islamic system.
   6.8. Publicizing illegal groups or parties.
6.9. Publication of government documents and material related to national security, the military or the police.

6.10. Publication of obscenity and immoral photographs and images.

6.11. Promoting use of cigarettes or drugs.

6.12. Libel against public officials and insulting real or legal persons.

6.13. Revealing private matters of persons and violating their personal sanctuary.

6.14. Publication of computer and information system passwords or methods to obtain such information.

6.15. Illegal commercial transactions through the Internet such as forgery, embezzlement, gambling, etc.

6.16. Buying, selling or advertising illegal goods.

6.17. Any unauthorized access to sites containing private information and any attempt to crack passwords or secret codes protecting systems.

6.18. Any attack on sites belonging to others for the purpose of disabling or slowing their operation.

6.19. Any attempt to intercept information over networks.

6.20. Creation of radio or television networks without the authorization and supervision of the “Sound and Vision” Organization [Sazeman Seda va Sima, which regulates Iran’s broadcast media].

The vague language of these provisions, particularly rules 6.1-6.9, drawn as they are from the 1986 Press Law and Penal Code, places unreasonable restrictions on free expression by effectively criminalizing any online criticism of the government.

Under rule 8, these prohibitions apply to Internet cafés and their patrons as well as to ISPs and their clients. In May 2001, the government temporarily closed more than 400 Internet cafés in Tehran.

…Between August and November 2004, the judiciary, led by Mortazavi in his role as chief prosecutor for Tehran, started a new campaign of arrests of journalists, nongovernmental-organization activists, bloggers, and the technical staff of Web sites specializing in political news. The authorities accompanied this crackdown with increased filtering and blocking of news and information Web sites and blogs inside and outside Iran.

In August 2004, the judiciary blocked the official Web site of the Islamic Revolution Mujahedin Organisation, Emrouz (http://www.emrouz.info), and the Islamic Participation Front’s Web site, Rooydad (http://www.rooydadnews.com). Both of these organisations represented reformist political forces with close ties to then President Khatami’s government.

On August 5, 2004, security forces detained Asghar Vatankhah, who was in charge of advertising on the Emrouz Web site. Three days later the authorities arrested a member of Emrouz’s technical staff, Masood Ghoreishi, who uploaded pages to the site.

The authorities detained contributing journalists and technical staff rather than high-profile political leaders under whose names these Web sites operate.
…Over the course of September 2005, researchers from Human Rights Watch and the Open Net Initiative (ONI), assisted by Iranian bloggers, tested 3,146 Web sites from Iran. Using the methodology described in the introduction to this report and in ONI’s other reports on Internet censorship around the world, researchers tested four categories of sites:

- A list of “high impact” sites reported to be blocked or likely to be blocked in Iran because of their content;
- A “global,” or control list of sites reflecting a range of Internet content, (including, for example, major news sites and sites about “hacking”);
- A list of Iranian blogs;
- Previous tests indicated that Web site filtering in Iran was likely accomplished by software called SmartFilter, produced by the U.S.-based Secure Computing. Secure Computing did not dispute these results at the time, but denied having sold the software to Iran. A fourth list, comprised of sites known to be blocked by this software, was included in this round of testing in order to test whether the government was still using SmartFilter to block Web sites.

In Iran, attempts to navigate to a blocked Web site immediately return a page saying that access to the site is “forbidden” or “denied.” The page varies depending on the ISP used (‘Iran’, in False Freedom: Online Censorship in the Middle East and North Africa 2005, Human Rights Watch, 14 November http://www.hrw.org/reports/2005/mena1105/5.htm – Accessed 13 May 2009 – Attachment 2).

An Open Net Initiative report on internet freedom in Iran, from May 2007, reports on a “Cyber Crimes Bill”, introduced to the Iranian parliament in 2006, which “makes ISPs criminally liable for the content they carry, effectively shifting the burden of censoring Web sites and potentially e-mail correspondence on to their shoulders”. The report continues to state that “ISPs that do not abide by government regulations (including filtering regulations) may be temporarily or permanently suspended, depending on the graveness of the offense, and their owners could face prison terms” (it should be noted that, as reported by Freedom House below, the cyber crimes bill never passed parliament, but another bill was introduced in 2008). In its conclusion, the report states that “Iran continues to maintain the most extensive filtering regime of any country ONI has studied”:

The Cyber Crimes Bill makes ISPs criminally liable for the content they carry, effectively shifting the burden of censoring Web sites and potentially e-mail correspondence on to their shoulders. Under the Cyber Crimes Law, ISPs that do not abide by government regulations (including filtering regulations) may be temporarily or permanently suspended, depending on the graveness of the offense, and their owners could face prison terms. Article 18 of the bill requires ISPs to ensure that “forbidden” content is not displayed on their servers, that they immediately inform law enforcement agencies of violations, that they retain the content as evidence, and that they restrict access to the prohibited content. The bill also includes provisions for the protection and disclosure of confidential data and information as well as the publishing of obscene content.

…IISPs and subscribers are also subject to prohibitions on twenty types of activities, where insulting Islam and religious leaders and institutions, as well as fomenting national discord and promoting drug use or obscenity and immoral behaviors, are prominent.

The Committee in Charge of Determining Unauthorised Sites is legally empowered to identify sites that carry prohibited content. Established in December 2002 (some reports state
June 2003), this Committee notifies the MICT of criteria for identifying unauthorised Web sites and what sites shall be blocked. The SCRC oversees committee members from the Ministry of Culture and Islamic Guidance, the Intelligence and Security Ministry, and the Sound and Vision Organization (Islamic Republic of Iran Broadcasting).

...However, not all filtering occurs through this body. The Internet Bureau of the Judiciary also orders ISPs to block sites through court orders, which are considered a form of lawful punishment imposed on legal entities. Tehran Prosecutor General Saeed Mortazavi, who has led harsh crackdowns on media and has also been implicated in cases of the torture of detainees, including twenty-one bloggers arrested in 2004, has also ordered that certain sites be censored. In May 2006 the MICT announced the formation of a central filtering office, reportedly to filter illegal content, identify Internet users, and keep a record of the sites they visit. The MICT subsequently denied having such tracking capabilities, saying its primary objective was to block pornography.

In 2001, the SCRC declared that the government was taking control of all access service providers (ASPs). ISPs were required to obtain bandwidth from these ASPs and also to employ filtering systems to block access to immoral, political, and other “undesirable” content while storing user data and reporting to the ICT Ministry. ISPs in which the government owns a share, such as the popular Pars Online, reportedly filter some sites at their own discretion over and above what is required by the regulations.

...Iran continues to maintain the most extensive filtering regime of any country ONI has studied. As filtering and censorship policies evolve, government officials and citizens have pushed back against many of the more extreme measures, including the ban on high-speed Internet in 2006. New developments may provide opportunities to contest these policies further. The draft Cyber Crimes Bill prohibits any blocking or investigation of data without a warrant issued by a court after evidence of suspicious activity. When this provision becomes law, it could potentially be used to impede the arbitrary closures and blocking of Web sites ('Iran’ 2007, Open Net Initiative website, 9 May http://opennet.net/sites/opennet.net/files/iran.pdf – Accessed 13 May 2009 – Attachment 3).

Radio Free Europe reported on internet freedom in Iran in November 2008, claiming that “authorities in Iran admit to blocking access to more than 5 million websites deemed immoral or antisocial”. The report states that “[a]ccording to Iranian law, every ISP must be approved by the Ministry of Culture and Islamic Guidance”; that “[t]hey are also required to install special filters to control the content of websites and e-mails passing through their network”; and that “ISPs that fail to comply with these rules face heavy penalties or closure. At least 10 ISPs in Iran have reportedly been closed for failing to install content-control software”:

Judicial authorities in Iran admit to blocking access to more than 5 million websites deemed immoral or antisocial.

Iranian media this week quoted Abdol Samad Khorram Abadi, an adviser to Iran’s prosecutor-general, as saying the country’s enemies “seek to assault our religious identity by exploiting the Internet.”

In reality, Iranian Internet users say, officials are mostly targeting independent news sources, as well as political, social, and music websites.

Iran is home to one of the largest populations of web users in the Middle East, with some 15 percent of the population having access to the Internet.
…Iranian authorities have introduced at least three sets of rules and regulations restricting the use of the Internet for readers, bloggers, and online activists, as well as for Internet cafe owners and Internet Service Providers (ISPs).

According to Iranian law, every ISP must be approved by the Ministry of Culture and Islamic Guidance. They are also required to install special filters to control the content of websites and e-mails passing through their network.

ISPs that fail to comply with these rules face heavy penalties or closure. At least 10 ISPs in Iran have reportedly been closed for failing to install content-control software.

In addition, every website in Iran is required to register with the Culture Ministry. A March 2009 report from Freedom House, titled Freedom on the Net: A Global Assessment of Internet and Digital Media, claims that “the Iranian regime wields one of the world’s most sophisticated apparatuses for controlling the internet and other digital technologies”. This report claims the existence of “at least a dozen ISPs in Iran, the largest and oldest of which, Pars Online, is partly owned by the government”, and that “many ISPs err on the side of caution by filtering more information than the government may actually require”. The Freedom House report notes that the 2006 cyber crimes bill failed to pass parliament, but states that a “different bill, introduced in July 2008, would make some cybercrimes – promoting corruption, prostitution, and apostasy on the internet – punishable by death. It passed its first reading with a vote of 180 to 29, with 10 abstentions, and was still under consideration at year’s end”:

Although Iranians are active readers and producers of online content, the Iranian regime wields one of the world’s most sophisticated apparatuses for controlling the internet and other digital technologies. Internet use in Iran began in 1995 at universities, then spread quickly via internet cafes to an otherwise isolated population with limited access to independent sources of news and entertainment. The government’s censorship of the medium did not begin until 2001, but users today operate in an environment that features filtering of content – particularly domestically produced political news and analysis – together with intimidation, detention, and torture of bloggers, online journalists, and cyberactivists. As with restrictions on press freedom that date to the early days of the 1979 revolution, the Islamic Republic couches its restrictions on internet freedom in an opaque and arbitrary conception of Islamic morality outlined by the constitution, the press law, and the penal code.

…The Iranian government restricts access and content through a mutually reinforcing set of decrees, legal regulations, and institutions. Supreme Leader Ali Khamenei first asserted control over the internet through a May 2001 decree and subsequent legislation by the Cultural Revolution High Council that forced all internet service providers (ISPs) to end their direct connections, obtain a license to operate, and purchase their bandwidth from government-controlled Access Service Providers (ASPs). There are at least a dozen ISPs in Iran, the largest and oldest of which, Pars Online, is partly owned by the government.

…Multiple government bodies deal with licensing and other regulatory issues. The Ministry of Islamic Culture and Guidance (MICG) is responsible for providing licenses for websites and blogs. The Committee in Charge of Determining Unauthorized Websites (CCDUW) is legally empowered to identify sites that carry forbidden content and report that information to the MCIT for blocking.
The Iranian government conducts some of the world’s most extensive censorship of online content, particularly on issues of political and social reform. Nevertheless, users circumvent filtering and make use of temporary openings in subversive, innovative ways. Both online and offline expression can draw punishment if it is seen as insulting Islam, criticising religious leaders and institutions, fomenting national discord, or promoting immoral behaviour. In late 2008, the government boasted of blocking five million websites, mostly for pornographic content, but also for sensitive political, social, and cultural information. Given the vague language of government blocking directives, many ISPs err on the side of caution by filtering more information than the government may actually require.

The Iranian government’s strategy for controlling internet content includes three general techniques: automated filtering, manually produced blacklists, and active posting of pro-government information. Automated filtering is enabled by SmartFilter, a commercial content-control software system developed by a U.S.-based firm, though company officials claim that the Iranian authorities are using it illegally and did not purchase it from them. All ISPs are required to install and utilise such government-mandated filtering systems. Automated internet censorship is supplemented by blacklists and blocking directives compiled by various unaccountable government bodies. At the end of 2002, the CCDUW was created to blacklist sites it deems anti-Islamic or a threat to national security. The committee consists of representatives from the Ministry of Information, the MICG, the Broadcasting Agency, the Cultural Revolution High Council, and the Islamic Propagation Organization. Its lists are regularly updated, and ISPs are required to adhere to them and restrict content accordingly, but the lists are not made public.

Iranian internet users suffer from routine surveillance, harassment, and the threat of imprisonment for their online activities, particularly those who are more critical of the authorities. The constitution provides for limited freedom of opinion and expression, but numerous, haphazardly enforced laws restrict these rights in practice. The 2000 Press Law, for example, forbids the publication of ideas that are contrary to Islamic principles or detrimental to public rights. The government and judiciary regularly invoke this and other vaguely worded legislation to criminalise critical opinions. A comprehensive 2006 cybercrimes bill would have made ISPs criminally liable for content on sites they carried, but it was never passed by the parliament. A different bill, introduced in July 2008, would make some cybercrimes – promoting corruption, prostitution, and apostasy on the internet – punishable by death. It passed its first reading with a vote of 180 to 29, with 10 abstentions, and was still under consideration at year’s end (‘Iran’, in Freedom on the Net: A Global Assessment of Internet and Digital Media 2009, Freedom House, 30 March http://www.freedomhouse.org/template.cfm?page=384&key=201&parent=19&report=79 – Accessed 13 May 2009 – Attachment 5).

One previous research response provides brief information on the internet in Iran, and it is provided as Attachment 6 (RRT Research & Information 2008, Research Response IRN33389, 29 May – Attachment 6).
List of Sources Consulted

Internet Sources:

Google search engine http://www.google.com.au

Databases:

FACTIVA (news database)
BACIS (DIAC Country Information database)
REFINFO (IRBDC (Canada) Country Information database)
ISYS (RRT Research & Information database, including Amnesty International, Human Rights Watch, US Department of State Reports)
RRT Library Catalogue

List of Attachments

1. ‘Internet Enemies – Iran’ 2008, Reporters Without Borders, 13 March


3. ‘Iran’ 2007, Open Net Initiative website, 9 May
