Refugee Documentation Centre (Ireland)
LEGAL AID BOARD

Iran - Researched and compiled by the Refugee Documentation Centre of Ireland on 5 August 2011

Information on internet freedom, in particular social media websites.

A report issued in May 2011 by *Freedom House* commenting on events of the preceding year notes:

> "Key international social-media websites like Facebook, Twitter, and YouTube were blocked after the 2009 election, and the list of disabled political sites continued to grow in 2010, hampering the opposition's ability to communicate and organize" (Freedom House (12 May 2011) *Freedom in the World 2011 – Iran*).

The *United States Department of State* reviewing events of 2010, note in a report published in April 2011 that:

> "The government monitored Internet communications, especially via social networking Web sites such as Facebook, Twitter, and YouTube, and collected individuals' personally identifiable information in connection with peaceful expression of views. The government threatened, harassed, and arrested individuals who posted comments critical of the government on the Internet; in some cases it reportedly confiscated their passports or arrested their family members (see section 1.f.). Freedom House and other human rights organizations reported that authorities sometimes stopped citizens at Tehran International Airport as they arrived in the country, asked them to log into their YouTube and Facebook accounts, and in some cases forced them to delete information" (United States Department of State (8 April 2011) *2010 Human Rights Report: Iran*, Section 2 Freedom of Speech and Press/Internet Freedom).

In April 2011 a document released by *Freedom House* states:

> "Since the protests that followed the disputed presidential election of June 12, 2009, the Iranian authorities have waged an active campaign against internet freedom, employing extensive and sophisticated methods of control that go well beyond simple content filtering. These include tampering with internet access, mobile-telephone service, and satellite broadcasting; hacking opposition and other critical websites; monitoring dissenters online and using the information obtained to intimidate and arrest them; ordering blogging service providers inside Iran to remove "offensive" posts or blogs; and trying to fill the information vacuum created by these measures with propaganda and misinformation" (Freedom House (18 April 2011) *Freedom on the Net 2011 – Iran*, p.1).

This report also notes:

> "As of December 2010, all the major international social-networking and media-sharing websites like Facebook, YouTube, and Flickr were blocked, while some file types, such as MP3 audio files, have been sporadically filtered. The periodic filtering and disruption of services based overseas—such as Google's fairly well-encrypted e-mail and blogging platforms, Gmail and blogger.com—appear designed to frustrate

users and eventually force them to seek more easily monitored alternatives based in Iran" (ibid, p.3).

It is also noted in this report that:

> "The Iranian authorities have taken a range of measures to monitor online communications and use them as a basis for criminal punishment. A number of protesters who were put on trial after the election were indicted for their activities on Facebook and Balatarin, a Persian site that allows users to share links and news. Many arrested activists reported that interrogators had confronted them with copies of their e-mails, asked them to provide the passwords to their Facebook accounts, and questioned them extensively on their relationships with individuals on their "friends" list. The authorities actively exploited the fear created by these reports, claiming that they had access to all the e-mail and text messages exchanged in Iran. The Computer Crime Law obliges ISPs to record all the data exchanged by their users for a period of six months, but it is not clear whether the security services have the technical ability to monitor all this data. In addition, ISPs have been accused of forging SSL certificates to eavesdrop on emails sent through secure channels (https), making protected communication increasingly difficult for those without more sophisticated skills" (ibid, p.7).

A report published in February 2010 by the *Institute for War & Peace Reporting* states:

> "Iranian police chief Brigadier General Ismail Ahmadi-Moqqadam recently warned the opposition that not only their text messages but also their personal emails were being monitored" (Institute for War & Peace Reporting (8 February 2010) *Sanctions Help Iran Limit Internet Use*).

The *Washington Post* in March 2010 notes:

> "…Iranian authorities have created cyber-intelligence units that are developing new methods to seek out and snare the opposition, including fake Facebook accounts" (Washington Post (10 March 2010) *Iran blocking Web sites in effort to curb anti-government activists*).

The *Iran Times International* in December 2010 states:

> "Iran's Intelligence Ministry has publicly admitted to something opposition activists have long suspected--hacking into opposition emails during last year's post-election protests" (Iran Times International (31 December 2010) *Regime openly admits reading opposition's emails last year*).

In December 2010 *Radio Free Europe/Radio Liberty* states:

> "Iran's Intelligence Minister Heydar Moslehi has publicly admitted hacking into the e-mail of opposition members. Moslehi was quoted by Iranian news agencies, including ILNA, as saying that e-mails were the most important tool of communication between opposition members during last year's postelection protests and that the Intelligence Ministry could break into them and defeat "the enemy." "(Radio Free Europe/Radio Liberty (27 December 2010) *Iran's Intelligence Minister Admits Hacking Into Opposition E-Mail*).

In June 2010 a document commenting on a student activist, published by the *International Campaign for Human Rights* states:

> "His email account was hacked after he was arrested last December, and it is now controlled by other individuals" (International Campaign for Human Rights (3 June 2010) *Fars News Fabricates Letter By Student Activist*).

The *Institute for War & Peace Reporting* in July 2010 states:

> "The term "Iranian Cyber Army" first emerged when a number of opposition websites abroad as well as Twitter and Baidu were hacked last year. Although the attack resulted in no more than a brief disruption of activity, the name and reputation were made – though what they refer to precisely remains unclear. No government agency has acknowledged control of the cyber army, but it is commonly believed that the Revolutionary Guards are behind it" (Institute for War & Peace Reporting (23 July 2011) *Cyber Wars in Iran*).

In November 2010 a report issued by the *International Campaign for Human Rights in Iran* notes:

> "A reliable source told the International Campaign for Human Rights in Iran that the fate of activist and Iran-Iraq war era deputy Islamic Revolutionary Guard Corps (IRGC) commander Mohammad Reza Farzin, remains unknown. Farzin was arrested two weeks ago by IRGC intelligence officers in Khorasan and transferred to an unknown location. The Intelligence Office of the City of Mashad disavowed knowledge regarding his whereabouts. Due to his heart condition, Farzin's arrest has gravely worried his family. Farzin had open heart surgery last year and also suffers from hypertension. The source who is close to the Farzin family, told the Campaign that nine intelligence officers of the IRGC stormed into Farzin's home without presenting a warrant while his wife and daughters were without their hejab, dressed in comfortable clothing, and eating breakfast. "The intelligence officers inspected family photos and videos of the former IRGC commander, obscenely looked through the wardrobes of his daughters, insulted him and his family, and, in a word, violated the sanctity of this religious family," the source said. "The IRGC officers took away all family members' mobile phones, a large number of books, personal computers, CD's, videos, and his family photos. They even hacked into his personal computer and gained access to his Facebook password, for the purpose of building a case against him by posting some non-religious contents on his Facebook page, which has been deleted since. The IRGC intelligence officers, some of whom he knows, searched his house for four hours," said the source" (International Campaign for Human Rights in Iran (4 November 2010) *Retired Revolutionary Guard Commander Arrested, Intelligence Officials Disavow Knowledge*).

References

Freedom House (12 May 2011) *Freedom in the World 2011 – Iran*
http://www.unhcr.org/cgi-bin/texis/vtx/refworld/rwmain?page=printdoc&docid=4dcbf51a39
(Accessed 4 August 2011)

Freedom House (18 April 2011) *Freedom on the Net 2011 – Iran*
http://www.unhcr.org/refworld/pdfid/4dad51b6d.pdf
(Accessed 4 August 2011)

Institute for War & Peace Reporting (23 July 2011) *Cyber Wars in Iran*
http://www.ecoi.net/local_link/143393/244154_en.html
(Accessed 4 August 2011)

Institute for War & Peace Reporting (8 February 2010) *Sanctions Help Iran Limit Internet Use*
http://www.unhcr.org/refworld/docid/4b7950ebc.html
(Accessed 5 August 2011)

International Campaign for Human Rights in Iran (4 November 2010) *Retired Revolutionary Guard Commander Arrested, Intelligence Officials Disavow Knowledge*
http://www.iranhumanrights.org/2010/11/farzin-arrested-whereabouts-unknown/
(Accessed 4 August 2011)

International Campaign for Human Rights (3 June 2010) *Fars News Fabricates Letter By Student Activist*
http://www.iranhumanrights.org/2010/06/fars-news-fabrication/
(Accessed 4 August 2011)

Iran Times International (31 December 2010) *Regime openly admits reading opposition's emails last year*
http://www.lexisnexis.com
(Accessed 5 August 2011)
This is a subscription database

Radio Free Europe/Radio Liberty (27 December 2010) *Iran's Intelligence Minister Admits Hacking Into Opposition E-Mail*
http://www.lexisnexis.com
(Accessed 5 August 2011)
This is a subscription database

United States Department of State (8 April 2011) *2010 Human Rights Report: Iran*
http://www.state.gov/g/drl/rls/hrrpt/2010/nea/154461.htm
Accessed 4 August 2011

Washington Post (10 March 2010) *Iran blocking Web sites in effort to curb anti-government activists*
http://www.lexisnexis.com
(Accessed 5 August 2011)
This is a subscription database

This response was prepared after researching publicly accessible information currently available to the Refugee Documentation Centre 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. Please read in full all documents referred to.

Sources Consulted

Amnesty International
Article 19
Committee to Protect Journalists
BBC News
Electronic Immigration Network
European Country of Origin Information Network
Freedom House
Google
Human Rights Watch
Human Security Gateway
Immigration and Refugee Board of Canada
Internal Displacement Monitoring Centre
International Campaign for Human Rights in Iran
International Crisis Group
International News Safety Institute
Iran Human Rights Documentation Centre
IRIN News
Lexis Nexis
Minority Rights Group International
Online Newspapers
Refugee Documentation Centre E-Library
Refugee Documentation Centre Query Database
Reliefweb
Reporters Sans Frontiers
Reuters
United Kingdom Home Office
United States Department of State
UNHCR Refworld