

# Iranian Internet Infrastructure and Policy Report

---

---

---

June - July 2013  
[www.smallmedia.org.uk](http://www.smallmedia.org.uk)

---

*This work is licensed under  
a Creative Commons  
Attribution-NonCommercial  
3.0 Unported License*



## INTRODUCTION

// In our previous, election edition of the Iranian Internet Infrastructure and Policy Report, we document the application and relaxation of controls on Internet connectivity and communications timed with the June 14 Presidential polls. Despite the introduction of new mechanisms to block tools used to bypass the filtering mechanism, by July the Internet had returned to its previous state of affairs that existed before February. From technical assessments and the reports of social media users, VPNs and circumvention software appears to operate normally for many, with specific restrictions still placed on the Tor network and unconfirmed reports of difficulties with Google's Android services and Viber. Conflicting accounts of blocking (and unblocking), most likely reflect the decentralization of some forms of filtering down to the level of ISPs. Whereas Parsonline may feel legally authorized to remove restrictions on VPNs, Shatel and others may not. This theme follows for throttling, outages, attacks against users and the sporadic reports of the unfiltering of social networks that have occurred across the month. Consequently, this report focuses on Iran, the politics leading up to the transition of presidencies after the election and the refocusing of the state on non-technical, legal means of policing content.

*Collin Anderson (Editor) and Small Media*

## CONTENT FILTERING AND BLOCKED SITES

**JUNE 29:**

The word 'gigolo' was reportedly blocked, causing incidental issues for Iranian Linux users attempting to install or update a similarly named software package used for managing network connections. [\(Source\)](#)

**JULY 2:**

The blog of Gholamreza Rajaei, an advisor to Hashemi Rafsanjani, was unblocked after 36 days. The site was initially blocked before last month's presidential elections for criticisms against the Guardian Council of the Constitution over the disqualification of Rafsanjani. [\(Source\)](#)

**JULY 4:**

The site for the Babylon translation and dictionary application was blocked. [\(Source\)](#)

**JULY 6:**

Internet users in the frontier city of Ahwaz reportedly experienced unstable Internet access.

**JULY 9:**

Tumblr was unblocked without any notice, however, users browsing the site are unable to see images since the domain used to host media (media.tumblr.com) remains filtered. [\(Source\)](#)

**JULY 12:**

Iranians reportedly experienced very slow connections to international sites. [\(Source\)](#)

**JULY 15:**

The filtering system was briefly offline across several ISPs, allowing users to access sites such as Facebook and Twitter. [\(Source\)](#)

**JULY 20:**

The official website of Molavi Abdul Hamid, a prominent spiritual leader of Iran's Sunni community, was blocked without any explanation. [\(Source\)](#)

**JULY 26:**

The site of the social network client [Hootsuite](#) was blocked.

**JULY 31:**

Irancell users report being unable to send text message containing slang phrases and sexual innuendo. [\(Source\)](#)

## POLICY DEVELOPMENTS

### **JUNE 30:**

Mehdi Akhavan Behabadi, the secretary of the Supreme Council of Cyberspace (SCC), stated that the video calling service on Rightel will be reactivated and that the SCC will consider giving permission to other operators such as Irancell for nationwide 3G services. Video calling feature was deactivated in May by the authorities due to cultural issues that was raised by some clerics. [\(Source\)](#)

### **JULY:**

eNAMAD.ir, an official department of Ministry of Industries and Business responsibly for controlling all online commerce, published a list of forbidden items that the online shop website cannot sell online. [\(Source\)](#). Please see [Appendix I](#).

### **JULY 8:**

The [Iran Post Office](#) (IPO) publicly announced the launch of own email service, claiming that all Iranians would be given an account. Users must register in person at the post office with their national identification and pay yearly fee (0.40 USD) to have access to 50MB per month. While the announcement brought international attention as the launch of 'the domestic email service,' the service has been active and available for at least early 2012. The press release also claims that the Post Office's platform was natively developed, however, all indicators point to the use of open source software, as with its competitors Chaapaar and Iran.ir, including the Roundcube webmail client. Researchers have noted the service's security holes originating from the use of an old, beta version of Roundcube. [\(Source: 1, 2, 3\)](#)

### **JULY 12:**

NIC.ir increased the fee for the registration of .ir domains by 10%, from 144,000 IRR (\$5.80) to 160,000 IRR (\$6.45). [\(Source\)](#)

### **JULY 16:**

The State Information Center announced that upon recommendation by several Ministries, the importation of telecommunication equipments will require direct authorization by the Ministry of Information and Communications Technology (ICT). [\(Source\)](#)

**JULY 17:** Mehdi Akhavan Behabadi announced that the SCC had studied a proposal to register all Internet users as a requirement for access. The purpose of this plan is to define different levels of filtering based on user need, for example differentiating the demands of the business sector from students. Also, Behabadi denied any plans to launch an 'Islamic Google Earth' or a 'Clean Internet,' and that Iranians would not be cut off from the global Internet. [\(Source\)](#)

### **JULY 25:**

The Ministry of ICT proposed a plan to organize local hosting service providers for security and limit the allowed companies to a set of government approved providers. [\(Source\)](#)

**JULY 27:**

Tehran Police conducted inspections of 352 Internet cafes as a part of a “a neighborhood security project” and shut down 67, citing various violations of city regulations against offering “illegal services.” [\(Source\)](#)

**JULY 30:**

The Twitter account of [Tehran Municipality](#) was verified by Twitter. It is the first governmental Twitter account inside Iran verified, despite the site being has blocked since the 2009 election. [\(Source\)](#)

## STATEMENTS FROM MINISTRIES AND POLITICIANS

**JUNE 16:**

Mahmood Liyaei, an adviser to the Ministry of ICT, announced Iran has 4 million Android users, accounting for 10% of the total Internet traffic of the country. [Cafe Bazaar](#), a locally developed app store, alone is responsible for 2% of the traffic. According to other statements by Liyaei, Iran’s mobile technology market is annually around \$4,000,000,000 (USD), divided evenly between phones and other devices. [\(Source\)](#)

**JUNE 26:**

Mohammad Hassan Nami, the head of the Ministry of ICT, announced that mobile 4G-based voice, video and data services will be launched by the end of next year (2014/2015). [\(Source\)](#)

**JUNE 28:**

Nami acknowledged that connection speeds were slowed in the lead up to the election by authorities for “security reasons.” [\(Source\)](#)

**JUNE 30:**

Behabadi noted that official VPN services would eventually be offered to individual clients. [\(Source\)](#)

**JULY 5:**

Ali Hakimi Javadi, Deputy Minister of ICT, stated that the telecommunications sector had successfully conducted at pilot program of providing high speed access to national network sites for home users (2 Mbps) and had requested last year that the SCC increase the regulatory limit. Government agencies have already ended their dependence on international access and have begun moving to a centralized database for sharing citizen’s data across ministries. [\(Source\)](#)

Behabadi, in an interview with IRIB, added that the main issue affecting the speed and price of access is price inflation by the Telecommunication Infrastructure Company, who buys access at 1Mbps for 15 USD to be resold to ISPs for over 100 USD. He added that the only way to solve this problem is privatisation of bandwidth providers in country. [\(Source\)](#)

*“Unfortunately, there is only one organization in Iran which is allowed to provide the necessary Internet bandwidth to local ISPs. There is not any competition in this field, and Telecommunication Infrastructure Company is a governmental organization. This type of pricing model is no longer acceptable, and I urge the officials of IT Ministry to revise the current guidelines in this regard.”*

(Source)

These statements were echoed later by Masood Riyazatian, Chairman of the Iranian ISPs Association. (Source)

**JULY 5:**

The Iran Cyber Police (FATA) of Tehran province announced the arrest of a 35 year old man selling VPN access. FATA noted that the suspect was found through “monitoring the web space.” (Source)

**JULY 9:**

Behabadi announced that more than 9,600 websites had produced 360 million posts against the regime and the elections. (Source)

**JULY 20:**

Mahmoud Khosravi, managing director of Iran’s Telecommunication Infrastructure Company, announced that only 26 companies had applied to use legal VPN services, despite a cost in the millions of dollars. Upon determining that the project was not sustainable, the TIC will reportedly not continue to offer it. (Source)

**JULY 22:**

Morteza Barari Qaem, Deputy Minister of ICT, noted that 50 Iranian search engines are active, with some having more than 50,000 visitors per day. (Source) Ali Eftekhari, head of Public Relations at the Ministry, said more than 8.3 million people connect with ADSL connections and the Internet penetration is 43%. (Source)

**JULY 22:**

MTN Irancell was forced to apologize after an SMS quiz was deemed insulting of a revered figure in Sunni history, Caliph Umar Ibn Al Khattab. The controversy evoked the attention of members of the Majlis and was deemed contrary to constitutional protections of recognized religious minorities. (Source)

**JULY 24:**

Mohammad Reza Aghamiri, member of the Commission to Determine the Instances of Criminal Content (CDICC), stated that Internet and SMS crimes during the recent elections was at a minimum level in comparison to previous elections. (Source)

**JULY 27:**

Saeed Salarian, deputy of the Supreme Council for Information and Communication Technology, said that Iran has restarted production of the filtering software for home and company users. This project was previously suspended due to financial problems. (Source) Behabadi commented that some websites are unintentionally blocked due to technical issues in the process of filtering. (Source) Additionally, the pilot phase of a new domestic antivirus product, “Padvish,” was announced, as well as the formation of a governmental effort to organize such efforts in order to compete with the international market. (Source: 1, 2)

**JULY 28:**

An official page for Ayatollah Ali Akbar Hashemi Rafsanjani was created on the Iranian social network Cloob. (Source)

## CIVIL SOCIETY, PROFESSIONAL ORGANIZATION STATEMENTS

### JUNE 29:

National Internet Development Management Center (MATMA) announced the Internet penetration according to each province, with a total rate of 61.06% and the top three most connected of provinces as Mazandaran, Tehran and Isfahan. (Source)

PROVINCE	THE INTERNET PENETRATION (%)
Mazandaran	83.85
Tehran	78.55
Isfahan	70.48
Khuzestan	68.04
Semnan	65.45
Qom	64.71
Golestan	63.48
Fars	61.33
Golestan	60.18
Khorasan, Razavi	59.24
Hormozgan	59.08
Yazd	57.56
Azerbaijan, East	57.13
Bushehr	56.39
Alborz	55.08
Chahar Mahaal and Bakhtiari	54.46
Qazvin	54.24

Hamadan	54.01
Zanjan	53.4
Zanjan	53.04
Markazi	50.9
Azerbaijan, West	49.86
Ilam	49.56
Kurdistan	48.35
Kermanshah	46.21
Kohgiluyeh and Boyer-Ahmad	45.09
Lorestan	43.89
Sistan and Baluchistan	41.77
Kerman	40.79
Khorasan, South	39.82
Khorasan, North	39.57

**JUNE 24:**

Pars Comtel, a high profile technology importer and partner to international companies such as Sony and Samsung, announced that they will no longer import mobile phones due to excessive fluctuations in local exchange markets. [\(Source\)](#)

**JUNE 30:**

Arash Iranmanesh, the regional Corporate Sales Manager of Kaspersky, stated that contrary to the rumors that began after Iran was removed from the company's site, Kaspersky had not ended business in Iran, that all products would remain supported and that a Farsi version would be launched. [\(Source\)](#)

**JULY 1:**

Majid Norhosseini, head of the Cyberspace Research Center, announced the **Parsijoo search engine** will be completed in the next 2 years and the first phase of localised OS, **Xamin**, will be finished soon. (Source)

**JULY 7:**

Rightel announced a partnership with Tehran Municipality to offer free Internet on local buses. (Source)

**JULY 15:**

Hamshahri published an article critical of the administration of the Internet, centered around four main problems: (a) slow speed connection, (b) repeated disturbances, (c) filtering of most websites, and (d) high price of the connection. The paper went on to criticize the announcement by the Post Office for failing to compete with foreign providers, noting that post.ir has existed for five years and is the third 'national email service.' (Source) Members of the Majlis's National Security and Foreign Policy Committee have claimed that they intent to investigate criticisms of the security of the national email services. (Source)

**JULY 21:**

Nasrollah Jahangard, former Secretary of the Supreme Council of ICT and special envoy for IT affairs under Khatami criticised the filtering regime's effectiveness in an interview, stating

*"At this time, social networking websites are available for clients in all the countries around the world. But the same service is blocked for Iranian users. Such types of measures reduce the trust of ordinary Internet clients to the activities of Iran Filtering Committee."*

(Source)

**JULY 24:**

A group of website owners and startups met with the Ministry of ICT to call attention to the limitation posed by slow connection speeds. (Source)

**JULY 29:**

Conflicting stories between the Iranian Ministry of ICT and satellite provider Thuraya exist over the source of delays in providing location information for three missing hikers, with the former blaming international sanctions. (Source)

# NETWORK ANALYSIS

//In this edition of the Infrastructure report, we have focused on the policy changes and discourses occurring immediately following the election of Hassan Rouhani. However, the unavailability of a consistent record of technical data on network conditions has remained a long-term concern the authors. In order to share data, we include the results of Netalyzer, a public tool for analysing the Internet path of a client computer. In the results contained herein from five prominent ISPs, we find significant structures used to intercept every most forms of Internet traffic, as well as direct blocking of communications services.

TCI DSL SERVICE	PISHGAMAN TOSEH ERTEBAT
<p>We detected the presence of an in-network transparent HTTP cache that caches data which was directly requested by the client.</p> <p>Weakly uncacheable data was cached between you and our server, even when the data was requested directly and explicitly. This suggests that there is an HTTP cache in the network which examines and caches web traffic. Since this content was not supposed to be cached, the HTTP cache is probably operating incorrectly.</p> <p>Weakly cacheable data was cached between you and our server, even when the data was requested directly and explicitly. This suggests that there is an HTTP cache in the network which examines and caches web traffic.</p> <p>Strongly cacheable data was cached between you and our server, even when the data was requested directly and explicitly. This suggests that there is an HTTP cache in the network which examines and caches web traffic.</p> <p>Your host, NAT, or firewall acts as a DNS server or proxy. Requests sent to this server are eventually processed by X.X.X.X.</p>	<p>The path between your network and our system supports an MTU of at least 1500 bytes, and the path between our system and your network has an MTU of 1450 bytes. The bottleneck is at IP address X.X.X.X. The path between our system and your network does not appear to report properly when the sender needs to fragment traffic.</p> <p>Your host, NAT, or firewall acts as a DNS server or proxy. Requests sent to this server are eventually processed by X.X.X.X.</p>

MOBINNET	MTN IRANCELL
<p>You are listed on the following Spamhaus blacklists: XBL PBL UDP access to remote DNS servers (port 53) appears to pass through a firewall or proxy. The client was unable to transmit a non-DNS traffic on this UDP port, but was able to transmit a legitimate DNS request, suggesting that a proxy, NAT, or firewall intercepted and blocked the deliberately invalid request.</p> <p>A DNS proxy or firewall caused the client's direct DNS request to arrive from another IP address. Instead of your IP address, the request came from X.X.X.X.</p> <p>A DNS proxy or firewall generated a new request rather than passing the client's request unmodified.</p> <p>Direct UDP access to remote SIP servers (port 5060) is blocked</p>	<p>Direct TCP access to remote SMTP servers (port 25) is prohibited.</p> <p>This means you cannot send email via SMTP to arbitrary mail servers. Such blocking is a common countermeasure against malware abusing infected machines for generating spam. Your ISP likely provides a specific mail server that is permitted. Also, webmail services remain unaffected.</p> <p>Direct TCP access to remote SIP servers (port 5060) is blocked.</p> <p>Direct TCP access to remote PPTP Control servers (port 1723) is blocked.</p> <p>Direct TCP access to remote DNS servers (port 53) is blocked. The network you are using appears to enforce the use of a local DNS resolver.</p>

DADEH GOSTAR ASR NOVIN (DGA)	
<p>Changes to headers or contents sent between the client and our HTTP server show the presence of an otherwise unadvertised HTTP proxy.</p> <p>The client was unable to send fragmented UDP traffic. The most likely cause is an error in your network's firewall configuration or NAT.</p> <p>The maximum packet successfully sent was 1452 bytes of payload.</p> <p>The client was able to receive fragmented UDP traffic.</p> <p>The following headers had their capitalization modified by the proxy:            Content-Type: text/html            Content-Length: 770            Last-Modified: Thu 07 Aug 2013 14:41:02 GMT            Set-Cookie: netAlizEd=BaR; path=/; domain=netalyzr.icsi.berkeley.edu            Connection: keep-alive</p> <p>The following headers were added by the proxy to HTTP responses:            Proxy-Connection: keep-alive</p> <p>The detected HTTP proxy changed either the headers the client sent or the HTTP response from the server. We have captured the changes for further analysis.</p> <p>The detected HTTP proxy changed images that were sent from our server.</p> <p>UDP access to remote DNS servers (port 53) appears to pass through a firewall or proxy. The client was unable to transmit a non-DNS traffic on this UDP port, but was able to transmit a legitimate DNS request, suggesting that a proxy, NAT, or firewall intercepted and blocked the deliberately invalid request.</p>	

## APPENDIX I

NO.	FORBIDDEN ITEM	NO	FORBIDDEN ITEM
1	Selling server	51	Selling morphine
2	VPN	52	Selling harmin
3	Illegal cosmetics	53	Selling LSD
4	Medicines	54	Selling cocaine
5	Sports supplements illegal	55	Selling Echinopsis Cactus
6	The satellite internet	56	Selling Golden Torch Cactus
7	Sexual accessories	57	Selling methamphetamine
8	Spying accessories	58	Selling crack cocaine
9	Weapons and ammunition	59	Selling hashish
10	Selling immodest movies	60	Selling teaching dance movies
11	Selling antiques	61	Selling sex education movies
12	Selling alcoholic drinks	62	Selling sexual accessories
13	Selling satellite	63	Selling marriage accessories
14	Selling firework materials	64	Selling erotic gum
15	Selling explosive materials	65	Selling sexual extender device
16	Selling flammable materials	66	Selling delay spray
17	Selling smoke bombs	67	Selling malware scripts
18	Selling erotic/sexy stories	68	Selling sending free SMS scripts
19	Selling illegal scripts	69	Selling Walkie-talkie devices
20	Selling LNB	70	Selling communication equipments
21	Selling [satellite] dish	71	Selling long distance phones

## Appendix

22	Selling satellite scissor	72	Selling Gin alcoholic drink
23	Selling satellite equipments	73	Selling any kind of alcoholic drinks
24	Selling sexual accessories	74	Selling pen with camera
25	Selling Marijuana	75	Selling Peyote cactus
26	Selling VPS	76	Selling grass
27	Selling SOCKS	77	Selling Whisky
28	Selling sexual medicines	78	Selling opium poppy
29	Selling tear gas	79	Selling latex sap of opium
30	Selling anesthetic gases	80	Selling Tramadol
31	Selling sexual dolls	81	Selling codeine
32	Selling any kind of shocker	82	Selling cannabis
33	Selling listening devices with sim card	83	Selling hemp
34	Selling microphone sim card	84	Selling Peyote cactus
35	Selling pen with camera	85	Selling snus
36	Selling watches with camera	86	Selling vodka
37	Selling buttons with camera	87	Selling opium poppy
38	Selling military handcuff	88	Selling drugs for increase /decrease of height
39	Selling baton	89	Selling drugs for increase sexual ability
40	Selling forbidden books	90	Selling obesity and impotence drugs
41	Selling crystal [drug]	91	Selling sexual tablets
42	Selling drug accessories	92	Selling sexual spray
43	Selling malware	93	Selling sexual gels
44	Selling SOCKS	94	Selling gambling equipments

Appendix

45	Selling circumvention tools	95	Selling grandes
46	Selling satellite card	96	Selling spray can cause nausea
47	Selling keylogger	97	Selling any kind of military sprays
48	Selling hacking software	98	Selling "Grediny "
49	Selling opium	99	Selling "Sky"
50	Selling heroin	100	Selling glasses with camera



