



access

AS IRAN BLOCKS VPNS, THE FIGHT FOR
THE INTERNET RUNS DEEPER

BY COLLIN ANDERSON AND FEREDOON BASHAR

*Collin Anderson is an independent researcher and Fereidoon Bashar is an Anti-Censorship Trafficker at ASL19.
Access is pleased to support and publish their analysis.*

INTRODUCTION

Beginning in late February, Iranians found their everyday outlets for communications for family and friends increasingly difficult to reach, subject to more expansive filtering by a government that has sought to impose one of the most extensive censorship regimes in the world. Even economic news and pro-government websites, such as the conservative news media Baztab and Tabnak, became the target of blocking and denial of service attacks, after unfavorable comments were left on the site by guests. For years, it had seemed the censorship regime and Internet users found a balance, while widely-popular social networking and media platforms would remain directly filtered, the informal economy for “filter shekan” (literally, filter breaker) would fulfill public demand for Facebook and YouTube.¹ When the government stepped on this implicit truce by first blocking access to the mobile messaging applications Viber and Whatsapp,² and then cutting off anonymity networks and circumvention tools, such as Tor³ and VPN,⁴ the reactions expressed by Iranians through blogs and alternative means to social media oscillated between derision, outrage, heartbreak, and dark humor. While the blocking of anti-filtering networks is worth international attention, Iran’s recent history of increasingly aggressive legal and technical restrictions on Internet users embody a more pernicious campaign against independent media sources that has real-world implications for the future of the country, especially at a critical political moment posed by upcoming elections in June 2013.

HISTORICAL CONTEXT

Amongst a wealth of other causes, international sanctions, ubiquitous corruption, and the tensions of a maturing generation, whose perspectives were not directly formed by the Islamic Revolution, have fomented an unpredictable political and social environment that continues to provoke the state to extend its campaign against online expression.

The recent blocking of anti-filtering tools and censorship of news sites follow a predictable but disturbing pattern -- when the political and economic situation of the country becomes unfavorable to the status quo, the government responds with an aggressive assault against the free flow of information. In late September and early October 2012, Iran underwent a series of systemic shocks, resulting from a devalued currency and the arrest of individuals associated with embattled political factions. These incidents were met with increased network censorship, including the blocking of foreign-hosted media files, jamming of international satellite broadcasts, and disruption of secure Google services.⁵ The widely-reported blocking of all SSL web traffic for several days in early 2012 coincided with the anniversaries of protests and the house arrest of reformist figures, Zahra Rahnavard, Mir Hossein Mousavi, and Mehdi Karroubi. Amongst a wealth of other causes, international sanctions, ubiquitous corruption, and the tensions of a maturing generation, whose perspectives were not directly formed by the Islamic Revolution, have fomented an unpredictable political and social environment that continues to provoke the state to extend its campaign against online expression.

1 <http://www.conovi.com/news-media/2012/12/17/over-half-of-internet-users-in-iran-use-facebook>

2 <http://nariman.me/?p=591>

3 <https://trac.torproject.org/projects/tor/ticket/8443>

4 www.reuters.com/article/2013/03/10/iran-internet-idUSL6N0C24M620130310

5 <http://smallmedia.org.uk/sites/default/files/reports/IIIP01.pdf>

While this seems to indicate an increasingly sophisticated use of the existing tools used to monitor and disrupt the country's networks, it also reflects the quiet formalization and coordination of the bureaucratic structures of electronic repression.

It appears that the recent blocking of the Tor network was accomplished through the use of deep packet inspection on nearly all connections made to hosts outside of the country. While this seems to indicate an increasingly sophisticated use of the existing tools used to monitor and disrupt the country's networks, it also reflects the quiet formalization and coordination of the bureaucratic structures of electronic repression.⁶ Domestic civil society, foreign governments and human rights organizations have taken notice of the growing role of these agencies in the policing of content and harassment of media, particularly since the violent death of blogger Sattar Beshetti.⁷ On March 11, 2013, the European Union designated Abdolsamad Khoramabadi under its financial and travel restrictions program against human rights violators, for his role as the head of the Commission to Determine the Instances of Criminal Contents (CDICC) and the Cyberpolice (FETA). At its creation the CDICC defined its authority as the ability to regulate and prosecute against any content it deemed against public morality and ethics, Islam and Islamic values, public security, authorities and governmental organizations, copyright, and invitation to commit other crimes.⁸ Under the justification, the EU notes both organizations' subsequent use of this nebulous mandate for the direct involvement in the repression of opposition sites, independent media, human rights material, and international communications platforms.⁹ Parallel actions were taken in early February by the US Department of Treasury against the IRIB, Iran's state broadcasting monopoly, as well as the Communications Regulatory Authority and Iran Electronics Industries, for using "state-media transmissions to trample dissent" through forced and false confessions.¹⁰ These lists created by European and American regulators begin to describe the complex bureaucratic structures established by the Iranian government solely in order to control access to information online and over-the-air.¹¹

While considerable attention has been given to the implications of plans for a "national information network," this rhetoric is a component of a broader campaign against the utilization of platforms outside of the government's physical domain and legal jurisdiction. In late January, Mehdi Akhavan Behabadi, the Secretary of the Supreme Council of Cyberspace, announced that the government will begin subsidizing domestic hosting services, including through decreasing costs at national data centers and other incentives, in order to encourage news sites to move their hosting to a domestic location.

While considerable attention has been given to the implications of plans for a "national information network," this rhetoric is a component of a broader campaign against the utilization of platforms outside of the government's physical domain and legal jurisdiction. In late January, Mehdi Akhavan Behabadi, the Secretary of the Supreme Council of Cyberspace, announced that the government will begin subsidizing domestic hosting services, including through decreasing costs at

6 <http://iranmediaresearch.org/en/research/pdf/file/1296>

7 <http://www.nytimes.com/2012/12/02/world/middleeast/after-death-of-sattar-beheshti-iranian-blogger-head-of-tehrans-cybercrimes-unit-is-fired.html>

8 <http://justiceforiran.org/human-rights-violators-individuals-databank/english-abdolsamad-khoramabadi/?lang=en>

9 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:068:0009:0013:EN:PDF>

10 <http://iipdigital.usembassy.gov/st/english/article/2013/02/20130206142214.html>

11 <http://www.hm-treasury.gov.uk/d/iranhuman.htm>

national data centers and other incentives, in order to encourage news sites to move their hosting to a domestic location. This is the latest initiative to follow last year's push to establish nationalized services for email, video sharing, social networking, gaming, and search. It also occurs in relation to four years of consistent, artificial throttling of connection speeds and frequent disruptions to international services, intended to discourage the use of foreign sites and stifle access to media resources, while falsely blaming well-known electronic attacks on the country's nuclear program.

The Iranian government appears to believe that it can follow the model of China, separating the economic benefits from a potential loss of social and political control. Shortly before the VPN blocking, Small Media Foundation in London described the then new requirement to register VPNs as a way of enabling the telecommunications regulators to block uncontrolled connections, without incurring the economic cost of shutting down international business transactions. The report foreshadows subsequent events by warning that "where the Supreme Council of Cyberspace promotes new policies on the registration of VPNs, we can expect that unregistered VPN connection will be blocked and throttled."¹²

However, despite funding made available by the state, by coercively forcing Iranians into domestic services, governmental policies directly result in the country trailing its neighbors in most measures of connectivity (such as broadband throughput and Internet penetration) and interference with basic communications activities of the public.

"I had a few other national emails as well and I tried all of them. But after two hours, I wasn't able to email a simple file using the Internet. I didn't intend to visit a certain website, and I don't use VPNs or other circumvention tools either. I wasn't going to download or upload a big file. I just wanted to send a simple email. An academic email."¹³

OFFLINE PARALLELS AND IMPLICATIONS

The government's assault on free expression and access to information has not been limited to filtering and electronic attacks against online media. The arrests of at least 17 journalists in late January, deemed "Black Sunday," and subsequent accusations of their cooperation with Western media outlets such as BBC Persian, were early signs that a crackdown on the press in the lead up to the 2013 presidential elections was in the works.¹⁴ Prior to the 2009 elections, the widely-assumed customary norm was that election periods would mean the brief relaxing of political and social restrictions, in order to increase public acceptance of the regime. Last year's Majlis elections, the first elections since 2009, brought its own series of arrests and censorship activities. These events and those of the past several months show that the political order of the country has shifted dramatically.

As the Iran Media Program wrote previously,

"[It] seems that for the upcoming elections, transparent debates, widespread public participation, freedom of press, and supporting the activities of various political factions are not the government's top priorities, although all of these have been used in the past to influence the voters. During the current election season, the government's most important concern seems to be protecting national security, avoiding political unrest and pre-empting actions to subvert violent protests."¹⁵

12 <http://smallmedia.org.uk/sites/default/files/reports/IIIP02.pdf>

13 <http://itna.ir/vdcepn8w.jh8nfi9bbj.html>

14 http://www.nytimes.com/2013/03/13/world/middleeast/un-rights-investigator-gives-harsh-appraisal-of-iran.html?_r=0

15 <https://asl19.org/en/irans-media-reality-crackdowns-and-journalist-detentions>

In February, Khorramabadi announced an expanded set of cyber crimes related to the upcoming presidential election. As Citizen Lab noted,¹⁶ these restrictions include publishing content that encourages the public to boycott the election, holding protests without special permits, interrupting the normal process of elections, or conducting any independent and unapproved media activity. Added to the list of cyber crimes were disturbing public opinion, spreading blasphemous material, publishing materials against the national interest, causing racial and ethnic conflict, and publishing the results of electoral polls. The state's control of the press, through requirements for registration, a legal monopoly on over-the-air broadcasting, and the economic impediments caused by the high price of paper against the low demand for advertisers, narrows the space for offline voices.¹⁷ In effect, Iran's official print and online media space is defined by the affiliations of outlets to particular political camps and popular figures, who are internally competitive but inevitably beholden to the state. When the government set out its new, long-term mandate for media and online crimes, it sent a clear message to the press, no deviation from the official line would be permitted.

MOVING FORWARD

Regulation of the internet is a rare topic in the political discourse of Iran where continual debate occurs over the role of the state and society in the freedoms of the individual and the development of the economy. The blocking of anti-filtering tools and the degradation of connectivity leads to negative reactions in the discussion and writings found in social networking sites, online media, and newspapers, and not only from reformist movements or persecuted groups. When the government attempts to exert more expansive controls on the internet, civil society and professional associations' defense of the internet is forceful. The strongest criticisms of the week-long blocking of Gmail came from professional associations and conservative bloggers. In an article posted on the Iran Technology News Agency site, entitled "Filtering Google and Points You Should Not Forget," telecommunications blogger Saeid Solemani wrote:¹⁸

"In that the growth and expansion of cyberspace and Internet carries with it dangers and consequences for users, there is no doubt, the entire world acknowledges and debates this, but the underlying concerns and fears caused by these in our country, are not the dangers, but [the communication's agencies] own shortcomings in improving security standards and development and use of virtual services and technologies."

"Lets look at this carefully: has this sort of control been successful in other cultural areas, to be successful where its control is even harder? Even more importantly, is the real danger, the use of this email service or something other? How is it that all the dangers that our children face in the Internet are forgotten and average users become targeted for restrictions. Users that when you block one way, will find a thousand other ways!"

As Small Media documents, such criticisms are not confined to particular political or religious factions. Conservative bloggers objected to the blocking of platforms such as Google+ and debated the blocking of Gmail, which was initially asserted to be in response to the Innocence of Muslims video. Majd al din Moalemi, wrote in a post titled "Filtering the thoughts of opponents":

16 <https://citizenlab.org/2013/02/middle-east-and-north-africa-cyberwatch-february-2013/>

17 <http://www.iranmediaresearch.org/en/blog/218/13/02/28/1281>

18 <http://itna.ir/vdcco4qi.2bq1s8laa2.html>

“By prohibiting Google, we have restricted ourselves and provided an opportunity to the opponents of civilisation. The best way to fight Google - who refuse to delete the video - is to share millions of messages, images and videos of the true lovers and followers of the Prophet Muhammad. It is necessary to send a wave of criticism and explanations to inform the public....But now they [the authorities] have cut off access to the necessary tools and have let the savages out. The opposition groups are able to circumvent filtering and access prohibited sites. Therefore gentlemen, try to comprehend this! By filtering social links, we are only restricting ourselves and leave the stage open to manipulations!”¹⁹

A year into the launch of a set of privately and publicly-developed national email services, which were pushed as answers to the security and economic needs of local users, these alternatives have failed to become viable replacements or attract a sizable audience.²⁰ These products were doomed from the start, being little more than open source email clients dressed up in an attractive theme, without attempting to appeal to anything more than the security threat provided to the government by Stuxnet. Moreover, the “China model” has clear limits. Iranians differ from Chinese audiences in their connections to the West and the country’s widespread diasporas; Iranians also came to depend on foreign services before national ones were offered. Unless local entrepreneurs can create products that fill the consumer demands unmet by international companies, the promises of domestic alternatives to foreign social networks and search engines remain an aspiration of the censorship policy of the state, not conducive to economic development and unlikely to appeal to the 20-30% of internet users who fueled an estimated 12 million dollar a year market for VPN services.²¹

It seems that the experiences of previous presidential elections leading up to and following the 2009 elections have changed the government’s policies and practices toward opening avenues for public debate and expression, online or offline. As much as international understanding of the power of social media is defined by Mousavi and Karroubi’s sophisticated use of internet platforms, so are the fears, regulatory policy, and tactics of those who seek to maintain the status quo. The disruption of VPNs will likely constitute only the start of more aggressive online and offline restrictions on freedom of expression and access to information, particularly if the government believes they are capable of imposing more significant outages with less economic collateral. This concern that the government is entering into a new phase of cracking down is mirrored in the recent rise of targeted malware and phishing attacks against civil society and media organizations, a particularly at-risk audience that is often left partially defenseless due to impediments in accessing antivirus software and security updates resulting from corporate compliance with American sanctions regimes.²²

There are more tools and opportunities for third parties to help than there were four years ago...we must keep in mind that the battles fought across the world to protect a free and open internet against overreaching governments resonate globally, and respect the centrality of Iranians themselves in the debate about censorship. These critical voices, as much as any international press or outside provided tool, have impeded the government’s plans for a more isolationist version of the internet, and create measurable political costs for interfering with communications.

19 <http://storify.com/smallmedia/iranian-conservative-bloggers>

20 <http://www.alexa.com/siteinfo/chmail.ir>

20 <http://www.alexa.com/siteinfo/iran.ir>

20 <http://www.conovi.com/news-media/2013/1/27/yahoo-leads-the-email-market-in-iran>

21 <http://itna.ir/vdcb5zb5.rhbfwpiuur.html>

22 <http://smallmedia.org.uk/content/82>

For those watching the censorship of the Iranian state from the outside, these affairs seem to be nothing more than disempowering. This, however, is far from the truth, there are more tools and opportunities for third parties to help than there were four years ago. Internet users have the ability to easily run censorship-resistant bridges for Tor,²³ foreign funders can continue to build on investments in the next generation of anti-filtering tools,²⁴ private companies are obligated to act on their responsibilities to protect the security of their users,²⁵ and governments must ensure that sanctions regimes do not interfere with access to connective technologies.²⁶ Finally, we must keep in mind that the battles fought across the world to protect a free and open internet against overreaching governments resonate globally,²⁷ and respect the centrality of Iranians themselves in the debate about censorship. These critical voices, as much as any international press or outside provided tool, have impeded the government's plans for a more isolationist version of the internet, and create measurable political costs for interfering with communications. The reaction of Solemani to the Gmail blocking frames the environment,

"Because they were unable to protect users against such threats and did not provide sufficient opportunities for social development so that progress in communication development is no longer a threat and danger, they are forced to consider the Internet as a threat and deal with it in such methods and ways that we see today. And then, refer to their accomplishments in support and protection of society with pride and in this way, consider themselves guardians of public safety and voice of society."

Access is a global movement for digital freedom premised on the belief that political participation and the realization of human rights in the 21st century is increasingly dependent on access to the internet and other forms of technology.

For more information, please visit www.accessnow.org or e-mail info@accessnow.org.

23 <https://blog.torproject.org/blog/obfsproxy-bridges-amazon-cloud>

24 <http://cima.ned.org/publications/empowering-independent-media-us-efforts-foster-free-press-and-open-internet-around-worl>

25 <https://www.accessnow.org/blog/2013/01/04/yahoo-bolsters-privacy-with-global-https-support>

26 <https://www.accessnow.org/blog/access-joins-open-letter-to-tech-industry-addressing-overcompliance-wi>

27 <http://jadi.net/2013/01/aaron-swartz-and-internet-azad/>

27 <http://www.iclub.ir/Aaron-Swartz-death>

27 <http://barsam.ir/archive/wikipedia-%D8%AF%D8%B1-%D9%85%D8%AE%D8%A7%D9%84%D9%81%D8%AA-%D8%A8%D8%A7-%D9%84%D8%A7%DB%8C%D8%AD%D9%87-sopa-%DB%8C%DA%A9-%D8%B1%D9%88%D8%B2-%D8-AA%D8%B9%D8%B7%DB%8C%D9%84-%D9%85%DB%8C-%D8%B4%D9%88/>

27 <http://khabaronline.ir/detail/194991/>

27 <http://www.itmen.ir/index.aspx?pid=10322&articleid=5210>

27 <http://www.mashregnews.ir/fa/news/93239/رابخاروسناس-ای-ی-دزد-ع-ن-م-ی-ارب-ی-نون-اق>