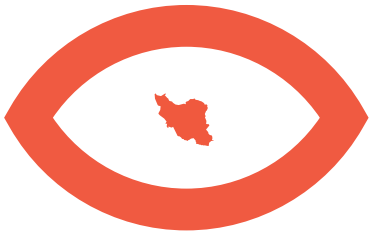
ARTICLE 19



Tightening the Net
Internet controls during and after Iran's protests

March 2018

ARTICLE 19
Free Word Centre
60 Farringdon Road, London
EC1R 3GA
United Kingdom

T: +44 20 7324 2500 / F: +44 20 7490 0566 / E: info@article19.org
W: www.article19.org / Tw: @article19org @article19UN
Fb: facebook.com/article19org

Contents

ARTICLE 19 recommendations

The Rouhani administration faces a number of challenges if it is to keep its promise to protect Internet freedoms and encourage innovation. ARTICLE 19 recommends as follows:

For the Information and Communications Technology Ministry:

- Cease policies that encourage the nationalisation of content and platforms for the purposes of controlling information flows;
- Cease the ICT Ministry's practice of giving discounts to those using local social media, in breach of the net neutrality principle;
- Engage with the judiciary and the National Security Council to end the restrictive approach to freedom of expression in Iran, especially in relation to its circumvention of processes and procedures to implement censorship and online controls;
- Ensure transparent documentation of censorship decisions, both through internal procedures, and from parallel organisations such as the judiciary and the National Security Council, and the Committee Charged with Determining Offensive Content;
- Answer to reports of violations to access, such as throttling (or slowing access) on Telegram; and
- To document and publicly share communications and negotiations with technology companies such as Telegram.

For the Supreme Council of Cyberspace:

- Cease existing censorship and threats to further censor platforms;
- Work with the National Security Council to ensure national laws and regulations in terms of Internet policy are followed, and end all arbitrary calls for controls based on 'national security'; and
- Stop encouraging the use of local platforms and instead encourage local development of technology without intimidation or violations of international standards on freedom of expression, including net neutrality.

For the judiciary:

- Recognise the right of Telegram channels and other bodies and individuals to seek, receive, and impart ideas and information of all kinds, regardless of frontiers according to Article 19 of the International Covenant on Civil and Political Rights (ICCPR) (additional regard needs to be paid to international human rights standards that condemn interruptions to access to information online);[1]
- Ensure full respect of international human rights standards, by conducting prompt, thorough, and impartial investigations into deaths in custody, all allegations of torture and other forms of ill-treatment, and cruel, inhuman, and degrading conditions of detention;
- Ensure due process in Internet decision-making by strictly following the procedures for implementing censorship online (notwithstanding the fact that Computers Crimes Law are in themselves problematic and need to be brought in conformity with international standards);
- Ensure the protection of the right to presumption of innocence, the right to a fair trial and due process;

[1] United Nations Human Rights Council (27 June 2016) *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development* A/HRC/32/L.20. Available from: https://tinyurl.com/yawdfnpy

- Implement the Criminal Code (Article 104) and the Computer Crimes Law (Article 48) when accessing information from prisoners;
- Denounce any practice by the Revolutionary Guards of sharing private information from people in custody with the state media in order to smear and influence their case (s) and compromise the use of criminal procedures[2]; and
- Work according to the highest standards of impartiality and always make decisions in full independence, notably from the paramilitary organisation of the Revolutionary Guards.[3]

For Iran's telecommunication industry:

- Decline to cooperate with government demands to cut off foreign traffic.

For foreign technology companies:

- Companies such as Telegram to provide documentation and be transparent regarding the Iranian government's claims of communication and negotiations with companies;
- Provide transparent explanations on how Telegram's Iran based infrastructure was affected during the period of censorship (regarding the content delivery networks (CDNs) that are based in the country); and
- Google must work to either attain a General License, or a Specific License under the Office of Foreign Assets Control regulations for services like Google App Engine in Iran.

For Iranian Internet users

- Use Iranian platforms for Telegram alternatives such as 'Soroush' with awareness that there is no privacy guarantee. Opt for alternatives such as Whats App, Signal, Wire, or iMessage. In times of heightened controls, seek safe circumvention tools to access communication tools over using Iranian alternatives;
- Make use of features such as 'ephemeral' or disappearing messages on platforms such as Signal, Wire, and Telegram to avoid carrying logs of communications or media that could help Iranian authorities incriminate you. On tools without these features, remember to delete old message logs;
- Practice digital hygiene as much as possible. Erase old invoices and documents from your email; and
- Never handover passwords to accounts. Utilise encryption technologies like PGP which will make the text of your communications on your emails illegible in case of takeovers by authorities.

[2] See Article 12 and 13 of the Islamic Penal Code from Iran Human Rights Documentation Center (IHRDC) https://tinyurl.com/ycxuhzdt . Article 12: Imposing and executing a punishment or security and correctional measures shall be carried out by a competent court and in accordance with the law and subject to conditions and requirements specified in the law. Article 13: Imposing and executing a punishment or security and correctional measures shall not breach the limit and conditions specified in the law or the judgment; and any loss or damage, if caused deliberately or negligently shall be followed by criminal and civil liability accordingly; otherwise, the loss shall be recovered from the public treasury.

[3] See open letter from human rights advocate Narges Mohammadi accusing the judiciary of being 'subservient' to the whims of the country's security agencies, including the Revolutionary Guards. https://tinyurl.com/y9j2zbsx

Key findings

- Internet shutdowns are still being implemented during heightened political mobilisation
- Controls focused on mobile connectivity
- No longer benign; the dangers of the National Information Network (NIN)
- The lack of process and procedure in censorship decisions, in dissonance with Iran's Computer Crimes Law and international standards
- Telegram's responsibility as a social media company
- Telegram's and Instagram's censorship in Iran
- Evidence of Telegram's throttling after the lifting of censorship
- Hardline and conservative elements encouraging a permanent ban on foreign social media
- Google's overcompliance with US sanctions proves to be a barrier to secure communications during protests for Iranians
- Unlawful seizure and dissemination of private communications and information of prisoners that violates Iranian privacy laws – the cases of Nazanin Zaghari-Ratcliffe and Kavous Seyed-Emami

Introduction

While this report comes as one of many in the *Tightening the Net* series, this is especially important as it outlines the concerning developments for freedoms online following the December 2017 to January 2018 protests that broke out across Iran. Our series of reports documenting controls online in Iran was born out of the policies which the last protest movement in Iran gave birth to. The 2009 Presidential elections and the ensuing 'Green Movement' catalysed Iran's Internet infrastructure, policies, and law towards increasing centralisation and control. While the cogs of Internet censorship and surveillance began to turn in the early 2000s with the boom of the Persian blogosphere, 2009 seemed to demonstrate the moment the government recognised the power the Internet had to mobilise the country, and ramped up effort to further control it. In the weeks leading up to the June 2009 elections, the momentum of the moderate candidate, Mir Hossein Mousavi's campaign convinced the government to block both Facebook and Twitter in May. Facebook had become the platform where Mousavi gained momentum in terms of support and organising; Twitter was the platform many outside of Iran used to stay abreast of the events. The legacy of these blockings remain to this day. Furthermore, on 13 June 2009, when election results were being announced, the government shut down the Internet for 45 minutes, and continued to slow down speeds after its reinstatement.

A series of events occurred after the movement settled down to codify this new tendency of the government to keep a hold of the Internet. The draft law of the Computer Crimes Law was first ratified by Parliament in 2008, however 16 days after the election, the sense of urgency pushed the law to be approved by the Guardian Council on 28 June 2009.[4] The law set in motion the normalisation of complete controls and repression online, along with the institutional procedures to implement censorship, through the decision-making body known as the Committee Charged with Determining Offensive Content (CCDOC) at the judiciary.[5] Other things that followed were the creation of the Supreme Council of Cyberspace, which centralised all the infrastructure, institutions, and decision-making of Internet policy to the office of the Supreme Leader in 2012.[6] Furthermore, the policing of the Internet was enabled through various bodies, including Gerdab within the paramilitary group of the Revolutionary Guards, as well as Cyber Police divisions within all of the country's police departments. Many awaited with concern during the ensuing elections to see what legacies of control would be enacted when the nation's citizens went to demand their vote. The 2013 presidential elections, however, demonstrated practices of some government throttling.[7] While arrests of those active online, such as Telegram channel administrators supporting Hassan Rouhani, were rounded up by the country's hardline elements (the Revolutionary Guards and the judiciary), overall disruptions online were minimal,[8] and the elections were seen as the first since 2005 where the Internet wasn't tampered with. However, many did not expect that mobilisation would not take the form of discontent during an election period, but would develop in the days following the

[4] Khabar Online (13 July 2009) *Iran's Cyberspace Criminal Law Was Announced* [in Farsi]. Available from: https://tinyurl.com/y7chb5gj

[5] ARTICLE 19 (2012) *Islamic Republic of Iran: Computer Crimes Laws.* Available from: https://tinyurl.com/ybyxb78h

[6] PressTV (7 March 2012) *Leader Decrees Establishment of Supreme Council of Cyberspace.* Available from: https://tinyurl.com/7xnsqex

[7] Anderson, C. (18 June 2013) *Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran* arXiv:1306.4361 [cs.NI]. Available from: https://tinyurl.com/y9jzksj6

[8] The judiciary disabled Telegram's voice call function when the platform introduced it in April 2017, in the weeks leading up to the election.

publication of the draft budget on 10 December 2017,[9] which continued to demonstrate the unequal distribution of the nation's funding among a population suffering from mass unemployment and economic inequalities. This report documents what has occurred during the protest period and their effects on law and policy. Many of these occurrences are a continuation of events documented in our previous reports. However, what is clear is that the seeds planted previously by the Rouhani administration, such as the National Information Network, can no longer be seen as benign after it led to the shutdown on international traffic that occurred throughout the protests. Additionally, the temporary ban on Telegram has set back the discourse of openings online that the Rouhani administration had promised to improve. One of the greatest achievements of the Rouhani administration in promoting Internet freedom was their defensive efforts to keep platforms like Instagram and Telegram uncensored against efforts of the more conservative and hardline elements of the nation. Efforts by the Rouhani administration to re-open platforms such as Twitter that have been blocked since 2009 seem more unlikely after the events surrounding Telegram. This paranoia that seems to drive tightening control over platforms after the protests is also leading to arrests and consequent unlawful treatments. However, we do not place all of the onus on Iranian authorities. We also highlight some inadequacies of companies such as Telegram and Google when making the Internet safe, secure, and accessible in Iran.

[9] Global Voices (9 January 2018) *The draft budget that inflamed protests in Iran.* Available from: https://tinyurl.com/ycv932hd

Censorship and access online

Net neutrality and the no longer benign National Information Network (NIN)

The National Information Network, sometimes referred to as the National Internet Project, has been studied in detail to look at its benign potentials for information and communications technology (ICT) growth in Iran, as well its ability to centralise Internet infrastructure to the hands of the government. In our first Tightening the Net report we documented the various phases of this project:[10]

- Phase one would separate the 'clean Internet' from its international counterpart;
- Phase two (planned for completion by 2013) would relocate all Iranian websites to domestic hosts; and
- Phase three, the final phase, would set up local management of the National Internet within the country, enabling total access and control by the authorities.

The case of net neutrality came to the fore with the government's aim to establish phase one and two. The government of Hassan Rouhani started to use various forms of incentives to lure Iranians to use local websites and applications over foreign online services. Since March 2017,[11] the government of Hassan Rouhani has placed pressure on internet service providers (ISPs) to provide incentives for users to access local content which has aided in the government's systematic efforts to censor the Internet. Unable to completely block access to censored websites such as YouTube, the government has resorted to providing pricing discounts and higher internet speeds to users who opt to use state-approved domestic versions of the site, like Iran's Aparat video sharing site, over foreign content.[12]

The dangers of this case became particularly heightened during protests, when connections to international traffic were being targeted. From 1 January 2018, users were reporting difficulties on various ISPs connecting to web traffic that was not hosted inside of Iran (see Figure 1).

Figure 1:

A user reports that his ISP provider, AsiaTech, does not allow him to access foreign web traffic on 1 January 2018. He explains he switched over to another provider, Irancell, to send out his tweet. A few hours later he posts the service has resumed back to normal.

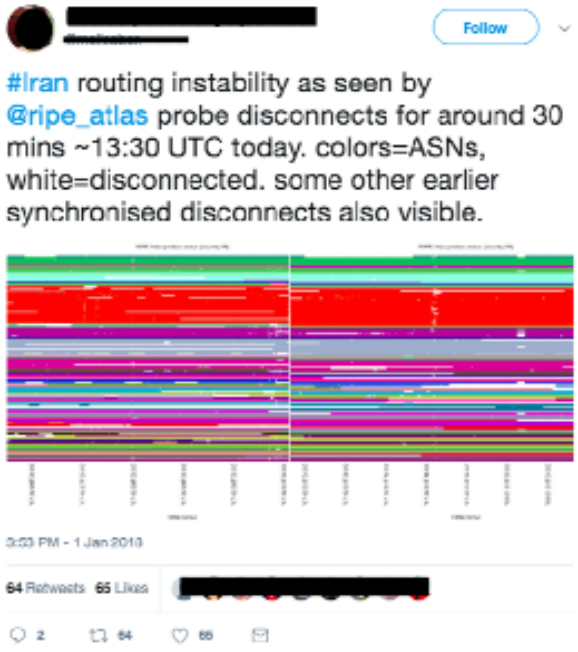
[10] ARTICLE 19 (29 March 2017) *Tightening the Net: The National Information Project.* Available from: https://tinyurl.com/y75xku2n

[11] ARTICLE 19 (July 2017) *Tightening the Net: Online Freedoms in Iran Following Rouhani's Reelection p. 6–7.* Available from: https://tinyurl.com/y7ot5kfj

[12] Joint statement by Campaign for Human Rights in Iran (CHRI) and ARTICLE 19 (21 December 2017) *US repeal of net neutrality harms Internet freedom at home and abroad.* Available from: https://tinyurl.com/ycpj6njf

A report by the Campaign for Human Rights in Iran (CHRI) found a source within one of Iran's seven Internet exchange points (iXP) who explained authorities had ordered them to interrupt international traffic. They told CHRI "every other international data packet is being bumped off the network, which creates widespread disruption."[13] User reports however were mainly explaining disruption on mobile connections. By 1 January 2018, users were soon reporting on inaccessibility issues to foreign traffic on both mobile and home connections (see Figure 2).

Figure 2:



Users who try to access sites with servers based outside of Iran are blocked from going online for 30 minutes according to Ripe_Atlas probes on 1 January 2018.

Concerns that decisions were adopted in violation of due process and the rule of law were raised when it became clear that they were imposed by various security agencies within the country working separately from processes set in place by Iran's official laws and protocols.[14] According to provisions of the Computer Crimes Law and the multi-agency body of the Supreme Council of Cyberspace, multiple authorities should decide together on such actions. Statements by the Minister of Information Communication and Technology, Mohammad Javad Azari Jahromi, later indicated the decisions were made by the Supreme National Security Council.[15]

The Case of Telegram

Discourses around Telegram and the 'evils' of Internet use

Hardline sentiments to control Telegram

Since its rise in popularity in 2015, Telegram has been the source of much debate and contention within Iran. From statements by Iran's Ministry of ICT that they were cooperating directly with Telegram, to sessions of the CCDOC convening to decide on whether or not the platform would remain blocked, with the country's hardline elements leading the urge to block the platform. In many ways, the Rouhani administration's ability to keep both Telegram and Instagram accessible, despite a history of the Iranian government's history of censoring popular foreign social media platforms such as Twitter and Facebook, had been their greatest Internet freedom victory.

Telegram was blocked on 31 December 2017 and reinstated on 13 January 2018. While the temporary block was in place, however, a number of hardline voices came to the fore regarding the necessity for such a control. An influential hardline cleric who leads Tehran's Friday prayers and is part of the Assembly of Experts, Seyed Ahmad Khatami, explained during the 5 January 2018 Friday ceremony:[16]

All of you saw the fire and catastrophe that cyberspace brought.

[13] CHRI (2 January 2018) *Iran's Severely Disrupted Internet During Protests: "Websites Hardly Open"*. Available from: https://tinyurl.com/y78butao

[14] An unnamed source told the Iranian Labor News Agency (ILNA) that an order to disrupt mobile connections had come from "higher officials in the security agencies". Available from: http://bit.ly/2BrgQ5a

[15] On 2 January 2018, ILNA quotes the Minister of ICT stating the disruptions are coming from the Supreme National Security Council.

[16] Khatami's Friday Prayer speech from 5 January 2018. Available from: https://tinyurl.com/y7xb8cvz

"You saw that when we closed down cyberspace sedition also subsided. Countries like China and Russia have introduced cyberspace [control] and have placed its management within their own hands. Why don't we bring the national Internet? ... Instead of this bizarre thunderbolt called Telegram. Do not say we've interrupted and need to come back again. Do not write and say we disagree with cyberspace, no; we agree with a virtual space when its keys are in the hands of the regime. "

Following the lifting of Telegram's censorship in mid-January 2018, a coalition of conservative Members of Parliament called for a ban on foreign social media applications.[17] The letter from 16 January 2018 addresses President Rouhani, Judiciary Chief Sadegh Larijani, and Parliament Speaker Ali Larijani. The MPs accuse foreign social media of promoting violence and drug use, as well as encouraging the protests and aiding the June 2017 Islamic State terrorist attack against Iran's Parliament and the Ayatollah Khomeini's mausoleum. The MPs also called for tighter controls on virtual private networks (VPNs), despite the fact that controlling VPNs proved to be an untenable task when President Mahmoud Ahmadinejad attempted a similar directive in 2012.[18]

In line with the sentiments of the MPs, the hardline chairman of the Guardian Council and Assembly of Experts, Ahmad Jannati, declared they must minimise and control the Internet on 25 January 2018, and explained the Supreme Leader was in talks with experts to understand ways to curb the "evils" of the Internet.[19]

During the ban in January 2018, Rouhani himself announced that social networks were closed down for a few days because "of the security situation". He however went on to reproach the hardliners, and their statements in support of making the ban permanent:[20]

"Now you want to abuse the situation and say things are looking good? That it should be closed forever? While you were comfortable sleeping, 100,000 people have become unemployed. Disconnecting online networks should not be permanent."

Despite the Rouhani administration's public statements in support of maintaining access to social networks, the fact remains that the Iranian government effectively closed the access to Telegram, depriving million of its citizens access to an established tool of communication and limiting their right to freedom of expression, despite their electoral promises and international human rights obligations. Other national initiatives also seem to contradict their statements. The administration did not broach the ongoing issue of removing the censorship on Twitter and Facebook, while declaring "disconnecting social networks should not be permanent". Additionally, during the press conference on 8 January 2018, while Rouhani expressed his seemingly liberal views towards the Internet, his administration's head of Digital Media within the Ministry of Culture and Islamic Guidance was announcing that they were working hard on a grand unveiling of a local platform that could function as an alternative to Telegram. We have extensively outlined the issues surrounding local platforms, their violations of privacy and net neutrality.[21] While not stated directly, it is believed the platform they were referring to was 'Soroush', a Telegram imitation application developed by the Islamic Republic of Iran Broadcasting (IRIB).[22]

The responsibility of Telegram

[17] IRNA Letter of 170 MPs in Iran's parliament calling for a ban on foreign social media. Available from https://tinyurl.com/yc94w6k4

[18] CHRI (18 January 2018) Majority of Iranian MPs Call For Ban on Foreign Social Media Apps. Available from: https://tinyurl.com/y8fu9dsg

[19] Jannati's 25 January 2018 statements. Available from: https://tinyurl.com/y7zo86ss

[20] Rouhani's 8 January 2018 Press Conference. Available from Fars News Agency's Twitter account: https://tinyurl.com/ybnowcmr

[21] Read about the shutdown of Cloob as an example of a failed local alternative and violations of net neutrality through promotion of local alternatives. ARTICLE 19 (November 2017) Tightening the Net p.3-4. Available from: https://tinyurl.com/y6vurhpf

[22] Read about Soroush, in Persian, on their blogs. Available from: https://tinyurl.com/y7x3ocfq

Telegram maintains around 45 million users inside of Iran and is widely seen as the central (private and public) communication platform for Iranians. These are significant numbers in a country with about 50 million users online (the population is around 80 million).[22] Telegram's public channels boast a wide array of topics, both political and quotidian, some of which are opposition diaspora channels, which ordinarily would be censored on other platforms, such as @sedaiemardom, which was previously known as 'Amad News' after Telegram removed it at the request of the Iranian government on 30 December 2017.

Figure 3:

Twitter exchange between the Minister of ICT and the CEO of Telegram to remove Amad News a day before Telegram's temporary blocking.

Previous ARTICLE 19 work has highlighted the concerns for a lack of transparency from Telegram in their relationship with Iran.[24] These concerns were heightened following Telegram's compliance with a removal request for Amad News[25] (see Figure 3). Telegram failed to illustrate the process and procedures behind the compliance, to much concern among digital rights advocates.[26] However, following heightened pressure and calls for due process and accountability, Telegram appears to have stopped responding to channel removal requests according to a 1 January 2018 statement by Durov, leading to the temporary block on the whole platform within Iran.[27] The blocking of Telegram coincided with a block on Instagram, another popular accessible foreign social media platform in Iran. While Instagram is not as central to communications and media as Telegram, Instagram is known to have about 24 million users in Iran.[28] Despite Telegram's refusal to comply, they have so far failed to respond to inquiries into how its content delivery network (CDN) located in Iran operated while the government placed pressure on the application and eventually blocked it.[29] Telegram must remain transparent on all its presence and relationships with the Iranian authorities.[30]

There was massive discontent across much of the country over the huge setback the blocking of Telegram was to everyday life, especially to businesses that rely on the platform. According to the Secretary of Internet Businesses Crafts Union, Reza Olfat Nasab, 100,000 licensed online sellers would lose their jobs across the country if Telegram were to remain blocked.[31] Needless to say, the block on Telegram contradicted many of the words and promises of both Minister Jahromi and the broader administration of Hassan Rouhani, whose ethos has always been to keep the Internet open, and to provide ICT development in order to enrich the economy. In a press conference about his report on "Citizens' Rights" just ten days prior to the blocking, Rouhani had declared "The space for people to communicate with the world will be maintained. We are not looking to filter social networks and the hand of our minister will not go over the filtering button."[32]

[22] Read about Soroush, in Persian, on their blogs. Available from: https://tinyurl.com/y7x3ocfq

[23] See statements by the CEO of Telegram Pavel Durov about the number of users inside of Iran. Bloomberg (12 December 2017) *This $5 Billion Encrypted App Isn't for Sale at Any Price.* Available from: https://bloom.bg/2AvursU. Latest statistics on Internet penetration in Iran in ITU (2017) *Measuring the Information Society Report 2017*. Available from: https://tinyurl.com/y7n77tsz

[24] ARTICLE 19 (September 2017) *Tightening the Net* p. 8 and p. 12, featuring concerns over Telegram's placement of Content Delivery Networks (CDNs) inside of Iran. https://tinyurl.com/y8uzr7n6

[25] Durov's 30 December 2017 statement on complying and blocking the 'Amad News' public channel. Available from: https://tinyurl.com/y83e4ozg

[26] Politico Magazine (1 January 2018) *What Telegram Owes Iranians.* Available from: https://tinyurl.com/ybn6ooey

[27] Durov's 1 January 2018 statement on Telegram's refusal to comply and its subsequent block in Iran. Available from: https://tinyurl.com/y7kkfkhk ; This was over the refusal to block Amad News' replacement, 'Sedaei Mardom'.

[28] This is a statistic from We Are Social (29 January 2018) *Digital in 2018 Global Overview.* Available from: https://tinyurl.com/yb7v6ka2

[29] Internet researcher Collin Anderson asked Durov publicly about Telegram's Iranian CDNs, without a response. See https://tinyurl.com/y887s7fe

[30] These were concerns we raised previously. ARTICLE 19 (July 2017) *Tightening the Net.* Available from: https://tinyurl.com/y7ot5kfj

[31] This is from Olfat-Nasab's interview in Al-Monitor in 12 January 2018. https://tinyurl.com/ybetsla6

[32] BBC Persian Report *The Fingers of Our Minister of ICT Will Not Go on the Filtering Button.* Available from: https://tinyurl.com/ydgtusx3

On 1 January 2018 however, Rouhani's Minister of ICT, Jahromi announced on his Twitter page (Figure 4):

Figure 4:

The Minister of ICT acknowledges his responsibility to keep cyberspace open for the economic opportunities they have promised to provide.

This translates as:

"One of the government's goals is to solve the unemployment problem and to develop new businesses and strengthen cyberspace. It's my responsibility to apologise to the hundreds of thousands of compatriots who have suffered from the recent conditions. We are negotiating with the Security Council regarding the restoration of peace and the removal of these restrictions."

This again echoes the same problems we found with the Internet shutdowns. Iran's own procedures, laws and regulations for implementing online censorship have been undermined and determined by the unelected body of the National Security Council.

Figure 5:

Iran's answer to Telegram, Soroush. With the same features of chats and public channels as Telegram.

Usage of Soroush after the Telegram ban

Again, hardline discourses indicated a different shift from others in Iran regarding the effects of the Telegram ban. Abdolsamad Khoramabadi, the head of the CCDOC, and the Deputy Prosecutor of the country, announced on his 'Soroush' channel (Figure 5), on 12 January 2018:

"Despite the proliferation of advertisement for the use of circumvention tools in order to bypass the Telegram block, Telegraphic [Telegram related] *activity on cyberspace has decreased by more than 90 percent. Within the short period of time that Telegram has been filtered, local social messengers such as Soroush, and iGap, have had tremendous growth in quality and quantity. If the Ministry of Communications, in carrying out its duties, removes some of the barriers to domestic messaging, they will soon achieve success and save the country from dependence on foreigners in this area. Investors and*

managers of native messengers, when they were convinced they could achieve unparalleled popularity from the people, they made significant investments in cyberspace in addition to using more specialists and employing more human capital, and investing in servers and hardware. But they need to be seriously support by the government in order to achieve their work."

There are a number of things to unpack in this statement. Firstly, on one of Iran's most popular application stores, Cafe Bazaar, Soroush has more than a million installations of its application,[33] while Telegram maintains more than 17 million installations from Cafe Bazaar.[34] Secondly, Khoramabadi's statements also contradict other indicators that showed while Telegram usage has declined, there remains a significant user base inside of Iran, with millions of posts and views having taken place during the block (not close to a 90% decline. See Figure 7 statistics from a Social Lab at the University of Tehran, also used by majazi.ir).[35] Thirdly, Khoramabadi's insistence that the Rouhani government is not working to promote local application development contradicts the facts, whereby this government has invested already in zero-rating policies and local alternatives. We outlined this extensively in the failures of the NIN to produce sustainable local alternatives, such as Cloob, that had to shut because of government censorship and monitoring demands (see pages 3-4 of the November 2017 *Tightening the Net* briefing).[36]

It is unclear whether ignorance is leading this dissonance between testimonies of individuals, such as Khoramabadi and Khatami, against those within the Rouhani administration.

Was the Government throttling speeds on Telegram after censorship?

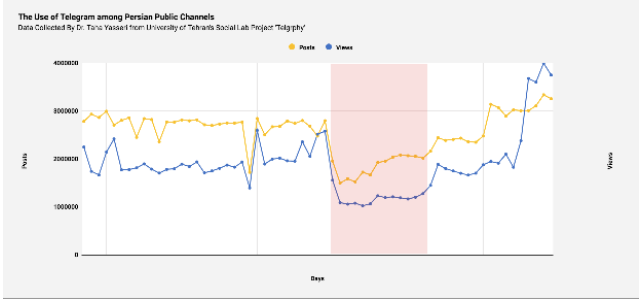
Once the block on Telegram was removed on 13 January 2018, user reports indicated slow connections over the application.[37] Durov confirmed this to be the case on the platform in a 15 January 2018 Tweet (figure 6).

Figure 6:

Telegram's founder and CEO, Durov confirms the reports of slower speeds on Telegram.

Data from the University of Tehran's social lab demonstrated that the number of posts on Persian public channels and the number of views on these posts struggled to resume to the same levels after the block was removed (the maroon area is the period of blockage). Levels only resumed to previous numbers around 20–21 January 2018.

Figure 7:

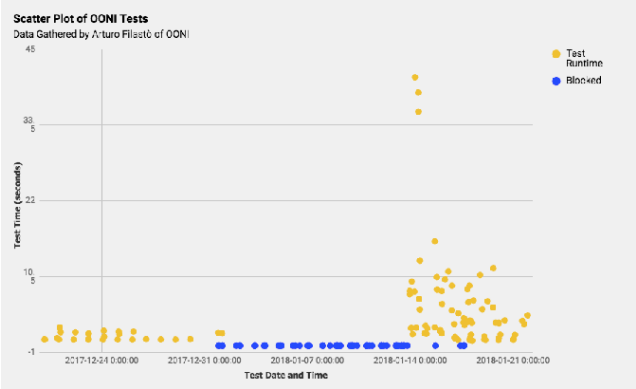


Yellow represents the amount of posts, blue represents the amount of views on posts. The section in pink represents the period where the blocking occurred from 31 December 2017 to 13 January 2018. The period following blocking appears to struggle to return to the levels of views and content shared on Persian Telegram channels. Previous decreases were caused by things like earthquakes. Data originally collected by Dr. Taha Yasseri.

[33] Cafe Bazaar installations of Soroush. Available from: https://tinyurl.com/ybk3d6w2
[34] Cafe Bazaar installations of Telegram. Available from: https://tinyurl.com/ybxtef7b
[35] Link only accessible from inside of Iran as of 20 February 2018. Available from: https://tinyurl.com/ybkuqo8x
[36] ARTICLE 19 (November 2017) *Tightening the Net: Online Openings and Closings in Iran.* Available from: https://tinyurl.com/y6vurhpf
[37] users reporting from Iran after the lifting of the ban on 13 January 2018 of slow download speeds on the application. Available from: https://tinyurl.com/ybheszt2

The test results from the Open Observatory of Network Interference (OONI), an initiative that uses probes to test the nature of Internet censorship around the world, noticed a slow return on test times when they probed for censorship results from the Telegram app and web version[38] within Iran (figure 8).

Figure 8:



OONI probes testing the Telegram app and Telegram web browser in Iran for blocks. The period after the block (the red dots that end when the censorship ended on 13 January 2018) shows slower connection speeds, correlating to statements by users, Telegram's CEO Durov, and other user statistics. Graph produced by Arturo Filasto, the co-founder and lead software developer for OONI.

Telegram itself has released no data in follow-up from Durov's 15 January 2018 statement, another drawback in their lack of transparency in documenting government interference in their platform. The data from the University of Tehran and the OONI probes are not exact science, however combined with the anecdotal users reports, there is a strong indication that authorities were continuing to limit the application's use after the ban was lifted, in further violation of access to Internet obligations that the Rouhani administration has made both in their promises and their international obligations. The government itself has made no official statements on whether or not they were throttling connections. Many users were still reporting that slow download speeds were posing hurdles to their business dealings. On 17 January 2018, Minister Jahromi tweeted that he was meeting with the Supreme Council for Cyberspace to coordinate their policy on digital economy, in the wake of the effects of filtering on businesses. Users started to question the Ministry's role in the slow download speeds, with no response from the typically vocal Minister (see Figure 9).

Figure 9:

Minister Jahromi on 17 January tweets: "After hearing from the Supreme Council of Cyberspace today, it was approved by the Ministry of Communications, with the formation of a working group consisting of the Minister for Economy, a deputy of the scientific community, with the presence of the National Cyberspace Center, will prepare within a month the document on the strategy of the Islamic Republic of Iran in developing the digital economy, and submit to the government for approval." In response, one of Jahromi's followers asked "Mr. Minister, is the Ministry of ICT deliberately slowing down the download speeds for pictures and films on Telegram?" obtaining no response.

The trouble with Google App Engine

Another accessibility issue that became clear during the protest period were the effects of Google's compliance with United States (US) sanctions in order to block the availability of the Google App Engine (GAE) in Iran. Mainly a concern for technologists and entrepreneurs who don't have access to the web framework and cloud computing platforms, it is often used by companies to host their websites and applications. GAE became crucial for circumvention however in December 2016 when the popular secure, end-to-end encrypted circumvention tool Signal started hiding its traffic through encrypted connections using GAE.[39] Signal has been known to be blocked in Iran since 2016,[40] however, this process, called 'domain fronting', did not make Signal accessible to users in Iran because Google has blocked GAE for as long as US sanctions against Iran have been in place. This became a concern during the mass arrests and incarcerations of protestors, with worries that detentions would violate the privacy rights of the detained during illegal interrogations. Signal features, such as disappearing messages and end-to-end encryption, become especially crucial as detentions and arrests often include seizures of devices and forced login into messaging logs and inboxes.[41]

This policy of Google is especially of concern given the GAE could be exempt from sanctions regulations under the US Office of Foreign Assets Control (OFAC) GL D-1,[42] under which Google could apply for an exemption for GAE's use in Iran. GL D-1, the personal communications General License, would be applied to GAE's use in facilitating domain fronting for tools enabling secure communications like Signal. While Signal's accessibility was removed once the filter on the platform was removed (see footnote 32), the wider issue of overcompliance on accessibility of Internet infrastructure in Iran is a continuing problem we have been documenting since the issue of Apple's removal of Iranian developed applications came to the fore in March 2017.[43] Google should seek a General License for these services in order to provide access to Iranians. Alternatively, if Google (along with other companies involved in hindering access for Iranians) does not think the General License can apply to their technology, they can apply to OFAC for a Specific License. For example, if a platform can be argued to have both personal communication considerations or commercial purposes, a Special License would provide a company with the authorisation to provide a particular service that essentially OFAC would not be opposed to being exported (i.e. we exempt all use of Google App Engine in Iran because it does not aid or further the nuclear programme).

[39] Open Whisper System, the organisation behind Signal, announced their 'domain fronting' method on GAE to circumvent censorship.

[40] See more on Iran's censorship of Signal in ARTICLE 19 (May 2017) *Tightening the Net* p. 5. Available from: https://tinyurl.com/ycef47pa . Reports from early January 2018 however indicated Signal was unblocked. Available from: https://tinyurl.com/y724eym5

[41] ARTICLE 19 (July 2015) *Computer Crimes in Iran: Risky Online Behaviour* p. 25. Available from: https://tinyurl.com/yajhby3q

[42] US Office of Foreign Assets Control (OFAC) GL D-1: https://tinyurl.com/jej8pmo

[43] ARTICLE 19 (September 2017) *Tightening the Net* p. 5. Available from: https://tinyurl.com/y8uzr7n6

Arrests and Intimidation

The period during and following the 2018 Iran protests has seen some of the most severe roundups of arrests since the 2009 protest period. Around 4,970 people have been arrested since the breakout of protests in December 2017. Issues of persecution and unjust prosecution are not new in Iran, however the lack of due process has come to the fore in the recent weeks, not only in how people are detained and prosecuted, but also in how devices are seized and the right to privacy is violated. Several cases that have gained publicity for access to personal information through these means are the cases of Nazanin Zaghari-Ratcliffe, the dual British-Iranian aid worker detained in Iran since April 2016, and the environmentalist and activist Kavous Seyed-Emami, who died while in custody in Evin Prison on 9 February 2018. In both cases Iran's national broadcasters publicised information, emails, and personal photos confiscated by authorities from the detainees in a way to designate them as foreign agents compromising national security.[44]

Zaghari-Ratcliffe and Seyed-Emami's cases are rare cases where confiscated digital documents were publicly aired in smear campaigns. However, these seizures are not unique, and not always used in the media, but rather in further prosecuting the detainees, or seeking other associated individuals for arrest. We previously documented this process in our 2015 "Computer Crimes in Iran: Risky Online Behaviour" report,[45] whereby intimidation is used to obtain information. The following is an analysis on how information is forcefully obtained from detainees, based on a series of interviews with over 25 respondents who had been prosecuted and detained by Iranian authorities for their online actions.[46]

Physical access to (confiscated) laptops and other devices

Examining confiscated laptops and other devices is the easiest way for authorities to extract information from detained persons. According to interviewees, it often happened that additional information gathered from their confiscated laptop computers further complicated their own cases after being arrested. In many cases, for instance, respondents only realised how much unprotected information they had saved on their computer devices after being arrested. This subsequently harmed them during prosecution. Often, respondents stated that had it not been for the examination of their confiscated devices, there would not have been enough evidence to sentence them.

The majority of respondents either failed to have a password, or had weak passwords for their online accounts on their electronic devices and/or personal computers. Often the respondent used a single password for multiple accounts, providing easy access for the authorities. One participant even admitted to having saved all their passwords to the desktop, owing to their poor memory. The use of password managers was never reported.[47]

Some respondents disclosed their passwords to the authorities immediately, thinking that they either had nothing to hide, or that they would be treated more leniently if they cooperated. However, interviewees who had acted in this way – in the belief that they would be treated less harshly by the authorities – found that they were mistaken.

In contrast, those respondents who did not volunteer their passwords to the authorities during interrogations, or who gave false passwords, managed to keep their accounts safe.

None of the respondents used encryption software on their

[44] See the Persian language film by IRIB from 14 February 2018 on Kavous Seyed-Emami here: https://tinyurl.com/y9cwuurb . See the English language film produced by the IRIB's English broadcaster PressTV from 6 December 2017 here: https://tinyurl.com/y8kv7bax

[45] ARTICLE 19 (July 2015) *Computer Crimes in Iran: Risky Online Behaviour.* Available from: https://tinyurl.com/yajhby3q

[46] See p. 25 of the above report. Footnotes from the original text have been removed from this excerpt.

[47] For further information on national policies on filtering and censorship and the role of ISPs, see OpenNet Initiative (16 June 2009) *Internet Filtering in Iran.* Available from: https://tinyurl.com/y8hvkw74

devices. In several instances, data found on the computers of people arrested led to the identification, compromise and (in one case in this study) arrest of other individuals. In one case, a respondent who had failed to delete their chat message history inadvertently revealed the identity of an individual who had been diligently deleting their chat history on their own device, and this revelation led to the arrest of the second individual.

Use of fragmented and incomplete intelligence

Fragmented intelligence gathered by the authorities from various sources was used as a means of intimidation, resulting in the individual surrendering more information about themselves in the (mistaken) belief that the authorities already knew everything about the arrested individual.

This method, reinforced by the pervading climate of fear in Iranian society, had an impact on the online behaviour of some respondents who believed that no matter how much they tried to be careful, the authorities already knew every detail of their lives. As a result they believed safety precautions to be useless.

Psychological pressure

Some respondents reported that the authorities threatened to share embarrassing private information about them unless they cooperated. Others reported that threats were made against their family members to put additional pressure on them. Family members were threatened by the authorities that their relatives would be treated harshly if they spoke out about their imprisonment. In various instances, the authorities made false promises to family members that if they cooperated and revealed information to the authorities, this would make it easier for their loved one in jail.

Torture and other forms of ill-treatment

Many respondents reported torture and other forms of ill-treatment being used by the authorities during their detention to force them into a confession. Respondents reported excessively long periods of interrogation, repeated beatings by law enforcement officers, slapping, verbal abuse, and being kept in detention conditions that could constitute cruel, inhuman or degrading treatment.

Interrogations as the primary source of information

All respondents were asked during interrogations for passwords and information about their contacts, networks, and the organisers of protests movements or gatherings. Some of the less high-profile respondents were asked to write down all they knew about certain friends, co-workers and other contacts. One interviewee stated that a 'large part' of their interrogation consisted of writing down all the information they had about every single contact detail stored on their mobile phone.

This latter method was typically used by the authorities when they had flagged an individual but lacked information and intelligence on them. This suggests that the authorities might not usually have the capability to access online accounts before arrest (apart from a few, infrequent cases of phishing), and therefore use arrests and interrogations as their primary means of gathering information.

Nazanin Zaghari-Ratcliffe

On 7 December 2017, Press TV, an English language branch of the Iranian state broadcaster IRIB released a documentary on Nazanin Zaghari-Ratcliffe's supposed work to encourage 'sedition' in Iran. The Press TV documentary was one in a series of documentaries aired in English and Persian by state media, but this one was aired on the eve of a new court case suddenly created to prosecute her a second time. It appears Iran's security officials extracted invoices and contracts Zaghari-Ratcliffe had accumulated in her emails regarding various projects she provided assistance or was involved in throughout her career.

Iran's information apparatus was studying the Zaghari case before her arrest. She was simply an English teacher in Iran, soon to start on journalism. Later she got a scholarship for communications management at England's Metropolitan University… a security organisation in Iran has given PressTV documents contrary to claims that she is just a mother in Iran. The said evidence shows she was a recruiter for BBC Persian service, targeting youngsters dissatisfied with the Iranian ruling body. She has also participated in other projects for British and US government affiliated companies to recruit and rank people. Her work with the BBC continued with a project called the ZigZag academy in a central call role. The BBC refrained from announcing her as an employee but her BBC payslip can be witnessed.[48]

Figure 10:

Images of documents PressTV claim to have acquired through security agencies – "documents contrary to claims that she is just a mother in Iran".

Further evidence from Zaghari-Ratcliffe point to the forcible handover of passwords and accounts while under duress after being placed in forced solitary confinement for over eight months, deemed as illegal interrogations that violate Zaghari-Ratcliffe's rights to due process and a fair trial.[49] She was arrested under the custody and orders of Iran's Revolutionary Guards, without judicial involvement or access to a lawyer, and forced to confess under duress.[50]

Forcible handover of digital access resulted in intelligence authorities retrieving invoices from Zaghari-Ratcliffe's emails. Authorities then misrepresented these as monthly salaries received from the BBC in an effort to smear her with fabricated roles and responsibilities related to opposition against the Iranian government. Furthermore, this forced retrieval resulted in their spreading of photos showing Zaghari-Ratcliffe without a headscarf to further smear her image as an agent of the west in Iranian media before her court appearance.

[48] Text transcribed from PressTV. Available from: https://tinyurl.com/y8kv7bax

[49] At the beginning of Zaghari-Ratcliffe's arrest, she was placed in solitary confinement, and transported 1000 km to Kerman, without any awareness of where she was, or any contact with legal counsel or family.

[50] BBC News (9 May 2016) *British-Iranian Nazanin Zaghari-Ratcliffe detained for a month "without charge".* Available from: https://tinyurl.com/z2sf6tr

A narrative of subversion against the state has been created through traces of projects and associations Zaghari-Ratcliffe maintained in her personal emails to organisations and projects the government saw as a threat. Violations of Zaghari-Ratcliffe's privacy and data in this instance were used to create propaganda against advocacy efforts to release her, and further justify the lack of due process and mistreatment afforded to Zaghari-Ratcliffe throughout her detention.[51]

Kavous Seyed-Emami

Kavous Seyed-Emami, a dual Iranian-Canadian national, was a sociology professor at Tehran's Imam Sadegh University, as well as an environmentalist running the Persian Wildlife Heritage Foundation. He was arrested alongside numerous other environmentalists in January 2018 in what Tehran's prosecutor said were arrests of people who had been gathering classified information under the coverage of "scientific and environmental projects".[52] Seyed-Emami's death in custody on 9 February 2018 was one of a series of suspicious deaths in custody of detainees following the recent wave of anti-government protests. Tehran prosecutor Abbas Jafari-Dolatabadi alleged with no proof that he committed suicide in a statement to ILNA news agency:[53]

He was one of the defendants in a spying case and unfortunately he committed suicide in prison since he knew that many had made confessions against him and because of his own confessions.

According to the Seyed-Emami family and lawyers representing them, there has been no medical report that can verify his cause of death.[54] Authorities have denied the family an independent autopsy. Meanwhile, the IRIB managed to air a documentary based on evidence it appeared intelligence services had extracted from Seyed-Emami's devices, online accounts, and physical raids of his family's home to extract private family photos, and benign communications with associates. One email between Seyed-Emami and a US friend was used in the documentary to conclude Seyed-Emami had ties with US intelligence arms, without any clear evidence or reason (figure 11).

Figure 11:

IRIB's 20:30 show airs a documentary smearing Seyed-Emami as a spy. Their evidence appears to be a seemingly benign correspondence between him and a contact named "David" that the documentary uses to prove Seyed-Emami's role as a foreign spy.

[51] See ARTICLE 19's call to end Zaghari-Ratcliffe's arbitrary detention. ARTICLE 19 (13 October 2017) *Iran: End arbitrary detention of media charity worker Nazanin Zaghari-Ratcliffe*. Available from https://tinyurl.com/ycfw5d9y. See protection of criminal procedure in Article 12 and 13 of the Islamic Penal Code from Iran Human Rights Documentation Center (IHRDC) https://tinyurl.com/ycxuhzdt . Article 12: Imposing and executing a punishment or security and correctional measures shall be carried out by a competent court and in accordance with the law and subject to conditions and requirements specified in the law. Article 13: Imposing and executing a punishment or security and correctional measures shall not breach the limit and conditions specified in the law or the judgment; and any loss or damage, if caused deliberately or negligently shall be followed by criminal and civil liability accordingly; otherwise, the loss shall be recovered from the public treasury.

[52] CHRI (15 February 2018) *Environmentalists Detained in Iran Denied Legal Counsel Weeks After Arrests.* Available from https://tinyurl.com/ybg3fxzo

[53] BBC News (11 February 2018) *Kavous Seyed-Emami: Iran environmentalist's death was suicide, Iran says.* Available from: https://tinyurl.com/yaek3gox

[54] CHRI (14 February 2018) *Lawyer: IRGC Film of Seyed-Emami's Prison Cell Does Not Show Act of Suicide.* Available from: https://tinyurl.com/y7kuxwux

Legality of documentaries including private documents

These two cases underline several worrying trends for the protection of human rights and fundamental freedoms in Iran, in particular the presumption of innocence, the right to due process and the right to a fair trial, as well as the right to privacy, as recognised under international human rights obligations. Firstly, that the work of security agencies that extract such evidence from the private communications and devices of detainees and create narratives of 'espionage' against these persons, is so readily accepted by Iran's judiciary and the IRIB undermines the presumption of innocence. Secondly, there is no respect for the fundamental rights of detainees. Article 104 of the Criminal Code specifies the following: [55]

In cases where there is a need to inspect and detect mailing, telecom, audio and visual correspondences related to the accused, in connection with investigation of a crime, the judge will inform the respective officers to confiscate [these materials] and send them to him or her. Once they are received, they will be presented to the accused, noted in the minutes, and attached to the file after being signed by the accused. Refusal of the accused to sign will be noted in the minutes and in case the items are not of relative importance, and if the confiscation is not necessary, they will be returned to the owner obtaining an acknowledgment of receipt.

The Computer Crimes Law points to a similar provision in Article 48: [56]

Surveillances of non-public and live content of communication in computer or telecommunication system will be dealt similarly to regulations of telephone surveillance.

Access to stored non-public content of communication, such as emails and text messages, is considered surveillance and related regulations must be observed.

As far as legal documentation for access to the devices and accounts of these two prisoners, the process and procedures are unclear. The evidence of the media narratives and adjudications so far prove that the aims and actions of Iran's intelligence agencies, namely the revolutionary guards, have been dictating the events of these cases, as opposed to any laws and regulations.

[55] Islamic Republic of Iran's Criminal Code of Procedure for Public and Revolutionary Courts. Available from: https://tinyurl.com/yaqanb43

DEFENDING
FREEDOM OF EXPRESSION
AND INFORMATION

ARTICLE 19
Free Word Centre
60 Farringdon Road, London
EC1R 3GA
United Kingdom

T: +44 20 7324 2500 / F: +44 20 7490 0566 / E: info@article19.org
W: www.article19.org / Tw: @article19org @article19UN
facebook.com/article19org