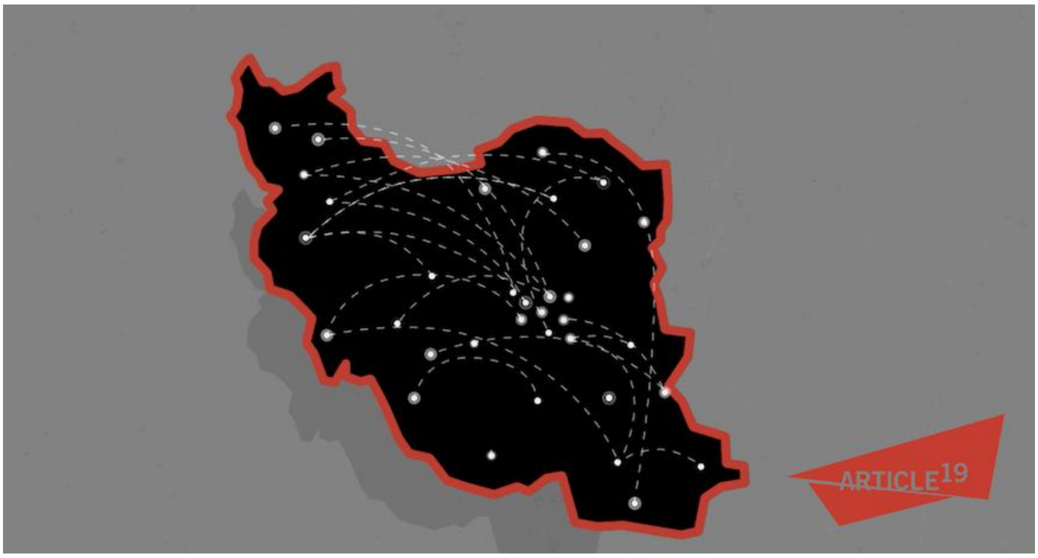
ARTICLE 19
(https://www.article19.org)

Tightening the net: Alarming moves to enforce the “User Protection Bill”



As part of ARTICLE 19’s ongoing monitoring work on the Iranian Internet, we’ve put together some updates of note, especially as the Iranian parliament moves closer to instating the concerning Internet Bill that we’ve been tracking (https://www.article19.org/resources/iran-parliaments-protection-bill-will-hand-over-complete-control-of-the-internet-to-authorities/). This brief was written by Sayeh Isfahani (https://slate.com/author/sayeh-isfahani), an advocate, journalist and Internet researcher with years of experience working in Iran.

Are we seeing the groundwork for the initiation of the “Protection Bill”?

In July 2021, the “Protection Bill” was tabled before the Iranian parliament under Article 85 of the Islamic Republic’s constitution. The article allows a select group of members of parliament to introduce legislation without it being debated on the parliament floor. Since then, there have been several incidents that have raised alarm and expectation that the Bill, which will usher in serious impediments to both access to the Internet and freedom of expression, will soon be implemented. Official remarks that the rollout of the draconian Bill will take place in March 2022 intensifies the need to campaign against it.

Some parliamentarians have also been making a number of statements indicating there is significant focus on putting the concerning bill into force. Recent months have seen user reports and evidence to indicate major slowdowns across Iran’s Internet connections.

And lastly, a scandal centred around an Iranian state-backed Instagram imitation application rocked Iran’s tech ecosystem, which encapsulated what the worrying nationalising elements of this Bill would mean once enforced.

Bandwidth Shortages: Reducing access to the international Internet in preparation for the Bill?

(https://www.article19.org)

Iranians have been reporting nationwide Internet disruptions (https://twitter.com/xhdix/status/1447860068871966720?s=20) since mid-September. Some users have even been facing trouble accessing basic services (https://www.zoomit.ir/tech-iran/375244-fixed-broadband-shortage-internet-problem/) like the Google search engine and email, along with Instagram and Wikipedia.

Others, in interviews with ARTICLE 19, have confirmed the presiding disruptions, adding that almost all censorship circumvention tools or Virtual Private Networks (VPNs or proxy services) have been either working with great difficulty or not connecting at all (https://twitter.com/SonitaSarabpour/status/1452537230317301764?s=20).

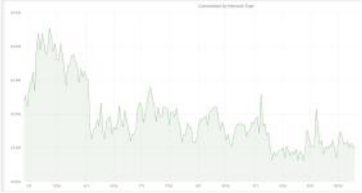


Figure 1: Psiphon connections through mobile networks (the most commonly used by Iranians to connect to the Internet) in Iran from 1 May 2021 to 25 Oct 2021 demonstrates a loss of users, especially throughout much of September.

Some government officials have blamed the disruptions on a sharp surge in demand for connectivity services after schools and universities reopened in late September.

Deputy Information and Communications Technology (ICT) Minister and head of the Communications Regulatory Authority Hossein Fallah Joshqani told the official Islamic Republic News Agency (https://www.irna.ir/news/84498681) on 10 October that demand for traffic was higher than usual owing to online school during the pandemic occurring at “peak hours”. Despite this reasoning, disruptions were reported outside of school hours.

The issue has even been discussed by government officials. Iran’s newly-appointed ICT minister Issa Zarepour acknowledged on 4 October the disruption (https://www.zoomit.ir/tech-iran/375044-slow-down-the-internet/) for the first time. Zarepour, who unlike his predecessor is not active on social media and only responds to text messages, answered a complaint by writing, “My colleagues at the Telecommunication Infrastructure Company of Iran [TIC] are working day and night to improve the quality [of Internet access].”

The TIC operates under the auspices of the Ministry of Information, Communications and Technology (ICT). It is one of the two sole providers of IP communications infrastructure to all private and public operators in Iran. On 4 October, Zarepour also issued an order calling (https://www.irna.ir/news/84493207) on heads of the Iran Communications Regulatory Authority (CRA) and the TIC to “immediately investigate” the cause of disruptions and publicly report measures taken to alleviate the issue. Such a report is yet to materialise. What is of particular significance, however, is that when the intensity of the disruptions reached its peak on 10 October, local technology website ZoomIt released an investigative report (https://www.zoomit.ir/tech-iran/375244-fixed-broadband-shortage-internet-problem/) that argued the disruptions were caused by “[international] bandwidth shortage” in the country. Local Internet Service Providers (ISPs) had told ZoomIt that the “quality of service[1] and data rate” of bandwidth provided by the TIC had declined significantly. The firms also had recorded recurring packet loss incidents in the network.

(https://www.article19.org)

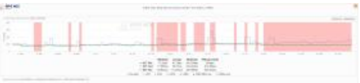
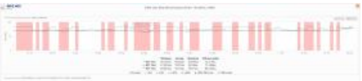
As per an unwritten mandate issued by Supreme Leader Ali Khamenei, Iran’s top cyberspace policymaker, the Supreme Council of Cyberspace (SCC), regulates purchase of bandwidth (https://www.zoomit.ir/tech-iran/375244-fixed-broadband-shortage-internet-problem/) from international providers. While acknowledging demand was exceeding supply, Deputy ICT minister Fallah committed (https://www.irna.ir/news/84498681) the TIC and communication operators to expanding their infrastructure to resolve the issues. However, he did not transparently indicate that the problem in actual fact lies with the SCC’s refusal to grant new licences.

According to ZoomIt (https://www.zoomit.ir/tech-iran/375244-fixed-broadband-shortage-internet-problem/), since Ebrahim Raisi took office as president in early August, the SCC has not issued permits for purchase of bandwidth from international providers.

In addition to contributing to the current bandwidth shortage, the shift in SCC policy is alarming since all bandwidth purchase contracts are dated, and the current deals will expire over time. If the Supreme Council of Cyberspace continues to refuse to issue purchase permits in future, the bandwidth connecting Iran to the international Internet will gradually shrink and further curtail access — a worrying step for the preparation of a Bill meant to radically reduce access and dependence on foreign Internet services.

Can VPNs explain the ongoing disruptions?

Although ARTICLE 19 tried to investigate data that supported the stated reasons for the strain and lack of bandwidth that led to packet loss on the network, we found the data did not necessarily corroborate this theory. While the Psiphon data we posted previously supported this doubt, we triangulated this with RIPE Atlas’ documentation of Iran’s network.

 Figure 2: The above is a graph that shows what kind of packet loss occurred across the AsiaTech network between 1 May 2021 and 25 October. For this particular ISP, we see more packet loss from August onwards, however for the past 6 months the occurrence of packet loss (pink highlights) seems often and not an anomaly.	 Figure 3: The above is a graph showing what kind of packet loss occurred across the MCI (or Hamrah Aval) network between 1 May 2021 and 25 October. For this particular ISP, we don’t see a particular point of packet loss (pink highlights). The loss is consistent across this period of time.

Figures 2 and 3 demonstrate what kind of packet loss was occurring across two major Internet Service Providers (AsiaTech and MCI/Hamrah Aval). There isn’t any consistent data to necessarily indicate the networks were suffering from the packet loss that the ZoomIt sources theorised were responsible for disruptions.

What can help us understand these disruptions or this problem of international bandwidth shortage could lie with what authorities are doing with VPNs and proxies, part of the cornerstones of draconian controls that characterise the “User Protection Bill (https://www.article19.org/resources/iran-parliaments-protection-bill-will-hand-over-complete-control-of-the-internet-to-authorities/)”.

An informed source told ZoomIt (https://www.zoomit.ir/tech-iran/375495-vpn-protocols-shutd[illegible]es-internet-slowdown/) that authorities are tampering with bandwidth for sp[illegible] internet protocols deciding to “manage network protocols one by one”. This type of reporting by the unnamed source implies that the decision has come from the top echelons of power such as the Supreme Council of Cyberspace, the Supreme National Security Council or other powerful security agencies. The source reported that with the aim of blocking censorship circumvention tools like VPNs and proxy services, network protocols (except 80 and 443 ports[2]) are being closely inspected. Finding out how VPNs and proxy services work is a hard task that requires inspecting the outbound and inbound data traffic of the country using extensive resources and labour.

The source explained these were technical maneuvres to prepare the groundwork for implementing the VPN ban for the Bill:

> *“Possibly, with the aim of implementing the Internet ‘Protection Bill’, and to detect ‘usual and unusual’ traffic, the country’s Internet [flow] is being intensely analysed. ‘Unusual traffic’ is traffic tunnelled through VPNs. The machines used for detecting the type of traffic cannot process this amount of data [simultaneously], and subsequently slow down the traffic, although bandwidth is available in abundance.”*

The source emphasised that application of inspection or detection methods significantly slow down the network since no single machine can analyse the whole bandwidth of a country simultaneously. Therefore, data packages get stuck in the line to be inspected one by one. This line of thinking is both corroborated by the decrease in users we’ve seen from Psiphon statistics (see Figure 1) — one of the most popular free circumvention tools available to Iranians. Below we can see connections and bytes (amount of traffic) across the two ISPs we were looking at through RIPE Atlas. While the RIPE data didn’t indicate necessarily network-originating packet loss, we are clearly seeing a drop in users and traffic across these two networks through Psiphon, meriting evidence to support the theory that disruptions are being caused by these VPN experiments.

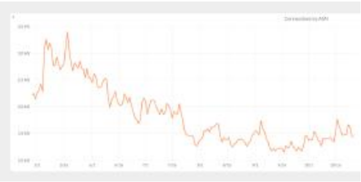


Figure 4: Here we see the amount of connections that were occurring across the MCI/Hamrah Aval network from 1 May 2021 to 25 October 2021, indicating a significant loss of users over time.

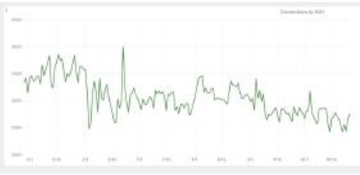


Figure 5: Here we see the amount of connections that were occurring across the AsiaTech network from 1 May 2021 to 25 October 2021, indicating some loss of users over time.

Updates on the Bill’s progress in Parliament: March 2022 expected for enforcement

Iranian MPs started reviewing (https://www.isna.ir/news/1400072618480) the controversial “Protection Bill” in a special commission on 17 October 2021. The Parliament’s Speaker Mohammad Baqer Qalibaf addressed the first meeting of the commission with his reassurance that the Bill would not curb Iranians’ access to international platforms like Instagram. He alluded that such allegations were part of nefarious agendas peddled by “specific groups” inside and outside of Iran. This claim however is woefully unsupported by the last publicly-available version of the Bill.

Qalibaf also vowed that the Bill will be reviewed in a transparent manner. Despite Qalibaf's ass[illegible] transparency regarding the Bill and its finalisation, Member of Parliament Ho[illegible] Nooshabadi noted that even the members of the specialised commission tasked with reviewing the Bill had yet to receive the most recent version of it.

(https://www.article19.org)

The commission has convened several times over the past few weeks. Under public pressure and despite initial resistance from MPs, the meetings have been streamed live (https://www.zoomit.ir/tech-iran/375535-parliament-plan-session-live/) on Parliament's official Instagram account (https://www.instagram.com/Ir_icana/).

So far, during the meetings, MPs have established the procedures (https://www.zoomit.ir/tech-iran/375649-broadcast-live/) for reviewing the Bill and are yet to start debating the legislation itself. Despite the meetings progressing slowly, Ali Yazdikhah, a member of the specialised commission, has said that (https://dgto.ir/2cz1) Parliament is aiming to ratify the Bill by mid-March 2022.

Rubika

A key component of the Bill is providing locally-developed services and platforms with financial aid and incentives through the establishment of a financial institution named "Fund for Supporting Local Key Online Services".

As per the Bill, the Fund's mandate includes investment in "purifying" cyberspace and promotion of "pure content in line with Iranian-Islamic values". The Fund is also charged with investing in "cybercrime prevention techniques". These appear to be euphemisms for investment in censorship and surveillance tools along with online propaganda and influence campaigns.

Investment in such projects has been a hallmark of the Islamic Republic's cyber policy. One such investment has led to development of a super-application dubbed Rubika, designed to replace Instagram.

On 14 August, news emerged on Persian social media (https://twitter.com/HumanGhorbanian/status/1426613924665962496?s=20) that Instagram accounts of prominent Iranian figures —including soccer players, movie stars and social media influencers— had been scrapped and Rubino accounts (a service of Rubika, which is a carbon copy of Instagram) were created for them without their knowledge or consent. Rubika had gone as far as giving some of the accounts a "verification badge" and reposting their photos onto Rubino.

After Rubika refused to remove (https://www.eghtesadonline.com/n/2met) the fake accounts, a campaign was launched on social media calling on people to report Rubika on Google's app market, Google Play. The campaign was successful, and Google banned Rubika (https://www.zoomit.ir/tech-iran/373826-rubika-app-removed-google-play/) on 19 August.

Iran's National Center of Cyberspace (NCC) condemned the Google ban (https://www.iribnews.ir/fa/news/3200457) on August 23, describing it as "monopolistic" and a "threat to [Iran's] sovereignty". The Center also threatened to ban Google in Iran if it does not roll back the restriction.

Considering Rubika's deep ties to the state, the NCC reaction did not come as a surprise for most people familiar with the company and its place within the broader plans of the "Protection Bill".

Rubiko’s deep-state ties

The app is developed by a state-linked tech company, Tooska, which is owned by Iran’s largest mobile operator (https://peivast.com/p/63086), the Mobile Telecommunication Company of Iran (MCI).

MCI is a subsidiary of Iran’s sole provider of landline telephone services, the Telecommunications Company of Iran (TCI).

The majority shareholders of TCI are Mobin Trust Consortium, with a 38.45% stake in the telecom giant, followed by the government, with 19.76%.

This ownership data is publicly available (http://www.tsetmc.com/) on the website of Tehran Securities Exchange Technology Management Co.

Mobin Consortium is controlled by the Islamic Revolutionary Guards Corps (IRGC) and the business behemoth Execution of Imam Khomeini’s Order (EIKO).

Both EIKO and the IRGC are in the tight grip of the Supreme Leader Ali Khamenei, as he appoints their top leaders and sets their policies.

The Bill underpins a history of corruption and nationalisation

The Rubika scandal was not the first time that tech companies with deep ties to the Islamic Republic misappropriated user data.

In a similar incident in May 2018, it was reported (https://www.bbc.com/persian/iran-44280722) that without people’s knowledge, accounts were created for them on local messaging app Soroush. The service was developed with extensive support from state-run Islamic Republic of Iran Broadcasting. In the face of mounting pressure, Iran’s National Centre of Cyberspace, the executive arm of the Supreme Council of Cyberspace, issued a statement (http://paydarymelli.ir/fa/news/35244) saying that it had “received no evidence” proving the incident had occurred.

The creators of locally-developed messenger apps and social media tools have often criticised the state for what they have described as “insufficient” support. On more than one occasion, the companies have also called on the state to strictly enforce censorship polices (https://aftabnews.ir/fa/news/535276). They argue that if access to foreign platforms becomes impossible, they will become popular. This is one of several startling cases the development of the National Information Network and the draconian realities the “User Protection Bill” is expected to force on Iranians.

[1] Quality of connection is called “Quality of Service” or QoS for short, in simple terms, means measuring the amount of data-loss in the connection: https://networkencyclopedia.com/quality-of-service-qos/

[2] In TCP/IP protocol, TCP Port 80 is dedicated to HTTP and port 443 is dedicated to HTTPS protocols: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers