FILTERWATCH YEARBOOK

THE STATE OFDIGITAL RIGHTS IN IRAN

1398

MARCH 2019 – MARCH 2020

FILTER WATCH

KAVEH AZARHOOSH, SIMIN KARGAR
MELODY KAZEMI, JAMES MARCHANT
JUNE 2021

CONTENTS

FILTERWATCH YEARBOOK 1398

PREFACE

WELCOME to the inaugural edition of the Filterwatch Yearbook. This is the first edition in a series of yearbooks documenting important developments shaping the Internet in Iran. The first two volumes of this report are being published in the early months of 2021, and cover the Iranian calendar year 1398 (which falls between March 2019 to March 2020) and 1399 (covering the period between March 2020 to March 2021).

We decided to start with our issue covering the Iranian calendar year 1398 as although over a year has passed since the reporting period, this was one of the most critical years in the shaping of the Iranian Internet. Iranian authorities imposed a major Internet shutdown in November 2019 in order to provide cover for a brutal crackdown on protesters, who had spilled onto the streets after a sudden announcement of an increase in fuel prices. This crisis shocked Iranians and the world, with the authorities' brutal response leaving at least 304 people dead, and many more injured or arrested.

Not all of the year's major developments were so visible, however. Iranian policy-makers also drove forward a number of important policy developments which we believe may shape the future of the

internet in Iran, and eventually result in a complex system of "layered filtering" in the coming years.

We have also chosen to put together these annual 'yearbooks' in accordance with the Iranian calendar given that many decisions, investments, and changes in policy are best monitored and understood in the context of the Iranian calendar year.

This report has been divided into two parts; the first will focus on policy developments, infrastructural changes, and practices by a range of actors which have shaped digital rights in Iran. We specifically focus on themes of surveillance, censorship, and digital inclusion.

In the second part, we have sought to contextualise these major themes and delved into how these developments affect the day-to-day lives of internet users in Iran. By taking a closer look at issues such as data security and media plurality we hope to emphasise the impact of Iranian policy-makers' decisions on the digital rights of Iranians.

Our aim is that this series will help digital rights researchers, human rights advocates, technologists, and those committed to advocating for an open, free and secure internet in Iran to better understand the ever-growing, complex and important realm of Iranian internet policy-making.

This report is the result of collaboration of the Filterwatch's research team, and includes contributions from Kaveh Azarhoosh, Simin Kargar, Melody Kazemi, and James Marchant.

The next issue of Iran's Internet yearbook – covering the Iranian calendar year 1399 (or March 2020 - March 2021) – will be published before the Iranian presidential election, which is set to take place in June 2021.

THE FILTERWATCH TEAM

THE CHANGING IRANIAN INTERNET & HOW WE GOT HERE

PART ONE

PART I

THE CHANGING IRANIAN INTERNET & HOW WE GOT HERE

THE Iranian Internet is endlessly evolving, and a number of major decisions shaping it were taken over the course of the Iranian calendar year 1398 (running between March 2019 - March 2020).

The first part of this report explores what these decisions were, how they were taken, and how they affected the development of Iran's internet infrastructure, information controls regime, surveillance systems, and online law enforcement practices. At the same time, we will explain why many of these decisions fundamentally undermine the human rights of Iranian internet users.

1 / INTERNET GOVERNANCE

OVER the last decade, we have witnessed an overhaul of internet governance and policy-making in Iran. With the establishment and development of the Supreme Council of Cyberspace (or SCC) as the country's leading policy-making body, and the increasingly assertive role played by the ICT Ministry and its subsidiaries, Iran is better-positioned than ever before to make and implement complex, long-term decisions about the ways that the Internet is governed.

This growing efficacy in policy-making has in no way translated to a commitment to upholding human rights online – in contrast, it has meant that Iranian authorities have been far more effective at making decisions about how to police the internet. Perhaps nothing is more demonstrative of this fact than the near-total Internet blackout that took place during the brutal crackdown on Iranian protests in November 2019; a shutdown that could only have taken place as a result of the state's successful development of the National Information Network (or NIN).

However, one advantage of this new policy-making regime has been a greater degree of transparency about the long-term aspirations of Iranian policy-makers. By monitoring the work of the SCC and ICT Ministry, digital rights activists can develop a stronger understanding of Iran's ambitions, and get ahead of forthcoming threats to digital rights in Iran.

Between March 2019 - March 2020 we observed worrying developments in Iran's policy-making bodies that clearly point towards further internet localisation (see **Section 2.1**), preparations for a "layered filtering" regime (see **Section 2.2**) and enhanced forms of information control (see **Section 2.3**). These measures, taken alongside the empowerment of law enforcement agencies to police online spaces (see **Section 3.2**) and continued barriers to digital inclusion (see **Chapter 4**), have seen the already vulnerable digital rights of Iranian citizens being further undermined during this period.

For more background on Iran's Internet governance structures, see Filterwatch's 2019 report *Bills, Bills, Bills: Upcoming Policy Challenges in Iran, and How We Can Resist Them.*[1]

1.1 POLICY DEVELOPMENT IN 1398

An Introduction to Iranian Policy-Making

Iran's policy-making processes have evolved in recent years to bring together a broad cross-section of Iran's political establishment. Currently, both the Supreme Council of Cyberspace (SCC) and Committee to Determine Incidences of Criminal Content (CDICC) are composed of different configurations of members

1 *Filterwatch*, "Bills, Bills, Bills: Upcoming Policy Challenges in Iran, and How We Can Resist Them", available at: **http://bit.ly/2vDloBk**

of Rouhani's Cabinet, representatives of the security establishment and the judiciary, and political appointees of Supreme Leader Khamenei. In this way, internet governance remains firmly concentrated in the hands of the SCC, CDICC, ICT Ministry, Judiciary, and law enforcement bodies. As we outline in this report, this policy-making structure has resulted in the SCC acting as the country's primary policy-making body.

Iran's governance bodies are designed to craft policy based solely on the interests of state-aligned stakeholders, and so are unable to effectively represent the needs and expertise of civil society organisations or Iran's growing technology sector. The limited interactions between these state bodies and the tech industry are largely limited to interactions with the (often state-supported) business and service providers who are instrumental in implementing the National Information Network project (NIN).

With policy-makers around the world struggling to grapple with the complexity of many challenges rooted in internet governance, many states have found that a multistakeholder policy-making process – engaging with industry and civil society – is a useful way of developing responses that are not solely designed to protect the interests of state authorities. The process in Iran, meanwhile, completely excludes civil society and the private sector from decision-making processes, resulting in the interests of state elites prevailing.

Lack of Transparency and Conflict

One result of the recent formalisation of ICT policy-making processes has been to (partially) open up access to formal documents, resolutions, and draft bills, helping us to better understand Iranian authorities' desired policy outcomes.

This said, there is an enormous need for the state to do more to open up its processes to public scrutiny. With no records published of SCC meetings, it is near-impossible for the public to gain insight into decisions that have been taken, or votes that have taken place. Only a few excerpts have been released to the public about significant resolutions, such as the Five-Year Plan for the National Information Network, passed in a February 2019 SCC meeting. This is not just a problem with the SCC; even in Iran's Parliament, records of MPs' votes are never publicly released, making it significantly harder for domestic digital rights activists to hold lawmakers to account.

Also, it must be noted that the four-year mandate of the SCC granted by Supreme Leader Ali Khamenei expired in September 2019. The council, whose membership and remit were designed by the Supreme Leader, had its current membership appointed in September 2015 for a four-year term. Since then, no decree has been issued for the council's renewal, despite its continued activity.

This lack of transparency is also on display when observing the workings of the CDICC and the Iranian Judiciary. The CDICC, which makes decisions about the implementation of filtering on a case-by-case basis, has been hosted

at the Judiciary since its formation in 2009. According to the Iranian Cyber Crime Law, 12 members of the CDICC should vote on decisions about the censorship of specific items of content. However, the committee has consistently failed to publish the records of its meetings and decisions that it has taken, making proper public scrutiny impossible (for more details on the role of the Judiciary and CDICC in filtering, see Filterwatch's past report on the subject).[2]

Following two years of silence, the Filtering Committee held an official meeting on 14 August 2019. Chaired by the Attorney General and attended by all of its members (minus two moderators appointed from the Majles), the Committee discussed the issue of providing "safe" internet access to filtered and restricted websites, based on users' individual and professional needs.

More conservative policy-makers have made similar complaints about being excluded from the policy-making process and SCC. According to media reports, former IRIB Director-General Ezzatollah Zarghami (and political appointee of the Supreme Leader to the SCC) was barred from one meeting by President Rouhani.[3] Rouhani and Zarghami publicly clashed on a number of issues, including over the January 2019 election of the new Chair of the Supreme Council for Cultural Revolution, Saeid Reza Ameli.[4]

2 Kaveh Azarhoosh, *Filterwatch*, 02/11/2018 "Understanding Iran's Emerging Internet Policy Agenda", available at: **http://bit.ly/3s8NHCP**

3 *Entekhab*, 16/04/2019, "Zarghami and the ban on attending two councils; where did the story begin?" [Persian], available at: **https://bit.ly/3d09Wqx**

4 Kaveh Azarhoosh, *Filterwatch*, 03/04/2019 "Saied Reza Ameli — The New Face Of Iran's Online Cultural Revolution", available at: **http://bit.ly/3qzzrml**

2 / INFORMATION CONTROLS

SINCE the Khatami era, Iran has implemented controls on the flow of information online. In the early 2000s, information controls and online censorship were largely limited to the filtering of specific URLs or keywords, but over the past decade Iran has developed far more sophisticated methods to influence user behaviours, and to make undesirable content less accessible.

In this chapter, we examine some of the latest technical and policy-related factors affecting Iranians' access to a free and uncensored Internet. Measures deployed in the last year included a near-total internet shutdown imposed in November 2019, the increasing regulation of the VPN market (potentially laying the groundwork for a new system of 'layered filtering'), as well as the introduction of new controls on SIM cards for specific user groups.

2.1 INTERNET SHUTDOWNS AND LOCALISATIONS

Iran's November/December 2019 Shutdown

Between March 2019 - March 2020 we observed two major internet disruption incidents. The first – a near-total internet shutdown – took place in November 2019, and was part of an incredibly harsh online and offline response to nationwide protests over a sharp hike in fuel prices.

The second disruption event in January 2020 followed the IRGC's shooting down of Ukraine International Airlines Flight 752, and was limited to localised disruptions of mobile data in Tehran. This disruption was seemingly an effort to interrupt the organisation and coordination of university students' protests.

But it was the first shutdown that proved the greatest threat to Iranian citizens, providing cover for a brutal crackdown that left at least 304 people dead, and many more detained by security forces, according to an in-depth report by Amnesty International.[5]

During this period, a near-total internet shutdown was enforced, restricting Iranians' access to the global internet via mobile internet connections and fixed-line services. As a result, users were almost entirely unable to access websites, services, and data hosted outside of Iran. However, users reported that some domestic services – those hosted on servers inside Iran – remained accessible.[6]

The blocking of access to the global Internet during this period offers clear insights into Iran's long-term aspirations for its information control apparatus, which seeks to expand access to sites, services and data hosted domestically

---

5 *Amnesty International*, 2020, "A web of impunity: The killings Iran's internet shutdown hid", available at: **https://bit.ly/3jPlNce**

6 Article 19, 2020, "Tightening the Net 2020", available at: **https://www.article19.org/ttn-iran-november-shutdown/**

– within reach of the Islamic Republic's governance systems – and limiting the country's dependency on foreign information and services offered from outside of the country.

Although Iran has been somewhat successful in using the internet shutdown to suppress reporting on the crackdown, and the tragic deaths that followed, the shutdown still proved costly for the economy. On 27 November, IRNA reported that the Commission for Digital Trade estimated that a 29,500bn IRR (approximately 70m USD) loss was suffered in digital and mobile payments during the internet shutdown.[7] According to unofficial reports provided by Payment System Providers (PSPs) inside Iran, there was a dramatic drop in online transactions during the first two days of the internet shutdown. In the following five days until the gradual reconnection of the internet, the number of online transactions stood at 48.5% of the transactions reported in the previous week.[8]

While the private sector suffered at the time of the shutdown, at least some key government and essential services still worked. In an interview with the tech magazine Peivast on 19 November Mehran Mahramian, the Deputy for Innovation at Iran's Central Bank, stated that disruptions to the Iranian financial system had been "mitigated" from the early hours of the shutdown, in collaboration with the ICT Ministry.[9] Mahramian confirmed that banking IP addresses were "whitelisted", and that the servers of banks and payment service providers were protected from network disruptions, being located inside Iran.

In the aftermath of the internet shutdown, when many individuals inside Iran voiced their strong anger at the decision, it became apparent that many policy-makers would seek to distance themselves from the decision. On 10 December the Qazvin, Alborz and Abyek MP Seyedeh Hamideh Zarabadi – who also sat on the Industry and Mines Commission – proposed a semi-urgent new bill seeking to prohibit internet shutdowns in times of national emergency, except when granted parliamentary approval.[10] The bill never gained approval to be debated, or voted on in the parliament.

Internet Localisation

The November shutdown proved that a number of Iran's key economic institutions could remain functional in the event that Iran is disconnected from the global internet, owing to their being hosted on domestic internet

7 *IRNA*, 27/11/2019, "2950bn toman damage to the Iranian economy during the days of the internet shutdown" [Persian], available at: **https://bit.ly/33RWSx2**

8 *Ibid*

9 *Peivast*, 19/11/2019, "Central Bank deputy: the internet shutdown poses no problem for banking networks" [Persian], available at: **https://bit.ly/2ZaWpnI**

10 *ISNA*, 10/12/2019, "Semi-urgent Bill on Access to Internet Services Handed to Heads of Majles" [Persian], available at: **https://bit.ly/3rQpGQO**

infrastructure. It is feared that the experience of this shutdown, and the perceived economic advantages of using domestic infrastructure (particularly in the event of another shutdown) may help to drive more Iranian companies to shift their services to the NIN, and host their data on domestic servers. Evidence from the last year also demonstrates that the state is actively encouraging such a shift, and is pursuing an aggressive policy programme of internet localisation.

The Supreme Council for Cyberspace (SCC) – which has been the leading policy-making force in shaping and driving the NIN and internet localisation over the last eight years – moved swiftly after the shutdown to facilitate even deeper forms of localisation. During two meetings on 1 February[11] and 15 February,[12] the SCC set a number of National Information Network (NIN) targets for 2026, with a focus on infrastructure development and the digital economy. Targets included:[13]

- 5% annual increase in "self-sufficiency" in the production of network equipment;
- 20% increase in the production of domestic mobile phones;
- The digital economy and online retail should make up 10% of national GDP;
- Basic digital economy services to be completed by 2021;
- Mobile internet access for 100% of the population, with an average speed of 10 MB/s;
- Broadband internet access for 80% of households with an average speed of 25 MB/s; and
- Internet speeds of 100 MB/s for businesses.

If delivered, these changes would help build resilience in Iran's digital infrastructure that could lessen any economic damage in the event of future internet shutdowns, therefore removing disincentives for their imposition, and posing a serious threat to the fundamental rights of Iranians. Many of the proposed SCC targets lay the groundwork for Iran to move to a layered filtering regime (see Section 2.2).

2.2 LAYERED FILTERING

Domestic VPN Market Marked for Tighter State Regulation

A significant section of the global internet remains inaccessible to Iranians, including sites and services such as YouTube, Twitter, and Telegram. Despite this, many of these sites remain popular in Iran despite only being accessible via circumvention tools such as VPNs.

---

11 *Majazi.ir,* 02/02/2020, "Approval of NIN objectives until 1404 in the Supreme Council of Cyberspace" [Persian], available at: **https://bit.ly/2ZboJGs**

12 *Majazi.ir,* 13/02/2020, "One of the fruits of the Islamic Revolution was to open space for women's activities" [Persian], available at: **https://bit.ly/32SLAJS**

13 *Ibid*

Iranians' deep reliance on VPNs to bypass state censorship has led governing elites, and in particular law enforcement agencies and the Judiciary, to demand further crackdowns on the availability of these tools.

Under pressure from the Cyber Police (FATA) and Judiciary to combat the availability of VPNs in Iran, on 26 October Deputy ICT Minister Hamid Fatahi reported that the Ministry had provided a list of online VPN vendors to the NCC, for further action.[14] Although many Iranians use VPN services provided by companies based outside Iran, a number of VPN providers based inside Iran still operate largely without interference from Iranian authorities.

Over the years there have been numerous discussions regarding the regulation of the sale of VPNs, although no concrete measures have yet been taken. It appears that by working towards the issuance of official licences to domestic VPN vendors, authorities aim to start mandating them to implement filtering policies, or else to force them to disable their services during politically sensitive periods.

VPN Regulation and the Drive Towards 'Layered Filtering'

Another function that such regulations may serve (if they materialize) is to introduce different levels of filtering for different user groups, or to establish a model of "layered filtering". Abolhassan Firouzabadi, the Secretary of the Supreme Council for Cyberspace (SCC) announced on 11 November[15] that the SCC "agrees with [the provision of] different levels of access to the internet" and that in relation to this, "we have made recommendations to the Commission to Determine Incidents of Criminal Content (CDICC)".[16] As part of this drive, "official" VPN providers will be established and regulated by the ICT Ministry, who will monitor their sale according to users' needs. New legislation regarding the legal and illegal sale of VPNs will also need to be implemented in order to regulate the Iranian VPN market.

Between March 2019 - March 2020 we did not see any formal documents or proposals regarding the planned regulation of VPNs. However, it appears that both the Judiciary and ICT Ministry have been asked to bring forward the necessary policies in the form of a bill or formal regulations.

"Layered filtering", then, refers to a policy championed by many Iranian policy-makers, with its objectives

14 James Marchant, *Filterwatch*, 15/11/2019, "Filterwatch – October 2019", available at: **http://bit.ly/3tZyUfJ**

15 *Mehr News*, 11/11/2019, "Official VPN operators established in the country" [Persian], available at: **http://bit.ly/3aQQ5Hy**

16 *Ibid.*

being to provide different groups of Iranian internet users with different degrees of access to information online. One example often discussed is to grant university students with greater levels of internet access than citizens. More information about Iran's layered filtering proposals are available in a previous Filterwatch report, linked below.[17]

The move towards layered filtering is in line with Iranian policy-makers' recent preference for less intrusive methods of information control. This subtler approach was is also on display in Iran's effective abolition of net neutrality in May 2017 when the Iranian ICT Ministry began charging users for foreign data consumption at twice the rate of domestic data.[18] This move meant that anyone who uses a VPN to protect their privacy and security online would also be charged twice as much for their data consumption. This not only discourages users from accessing foreign content, but also discourages them from practising basic online security and safety measures.

Another recent example of Iran's movement towards layered filtering has been the introduction of SIM cards specifically for minors (aged 6-18). The scheme, which is supported by the ICT Ministry and leading mobile operators, provides SIM cards to minors in Iran with extremely limited access to the internet. The SIM card only connects to white-listed services and content deemed appropriate for minors. Users of these SIM cards do not have access to internationally hosted content. Currently RighTel Communications and the Mobile Telecommunication Company of Iran offer these SIM cards. According to ICT Minister Jahromi, as of 1 January 2019 1.5 million of these SIM cards had been distributed to families in Iran.[19] For more information on this scheme, see **Section 4.1**.

2.3 CONTENT FILTERING

Streaming Sites Latest Target of Filtering

Since the vast majority of popular foreign websites have already been banned, the coverage period saw fewer high-profile incidents where major foreign sites were filtered in Iran. One major incident during this period was the order by Javad Javidnia, the interim chief of the Judiciary's Cyberspace Department, to block Google Play. On 9 October 2019, the Judiciary sent a formal letter to telecommunications service providers ordering them to block

17 Kaveh Azarhoosh, *Filterwatch*, 19/09/2019, "Is "layered filtering" the future of Iran's National Information Network?", available at: **http://bit.ly/3s55pqV**

18 *IRNA*, 7/03/2017, "Separating domestic and international internet [traffic] with the aim of strengthening the national information network" [Persian], available at: **http://bit.ly/3k0fliJ**

19 *ISNA*, 01/01/2019, "Remove all American products from the NIN" [Persian], available at: **http://bit.ly/3agwrG1**

the official Android app store Google Play "as soon as possible".[20]

There have also been occasional incidents in which domestically hosted sites have been filtered. On 3 October 2019, Mehr News reported that a number of Iranian websites offering free movie downloads (such as Tiny Moviez) had been blocked.[21] Following complaints by the public, Jahromi went on to tweet that the decision originated from the Judiciary, and that he had no involvement in it.

It was later reported that the move was taken to protect the intellectual and material property rights of content creators. Other state news outlets have reported that that the Judiciary's decision was motivated by complaints from other fee-based streaming services such as Filimo, and to reduce competition for domestic service providers.[22] This decision was not explained by the Judiciary.

As noted earlier, the blocking of foreign websites are often bypassed in Iran using circumvention tools. The arguably unsuccessful ban on Telegram has demonstrated the limitations of content filtering strategies in Iran (and is perhaps one of the reasons for the pushing of other means of information control, such as Layered Filtering). Nonetheless, Iranian officials have continued to warn against the use of banned tools and websites. For instance, Fars News reported on 28 February that Javad Javidnia, Iran's Deputy Prosecutor for Cyberspace, made a statement reiterating the enforcement of the ban on the use of foreign messaging apps, specifically by schools, universities and government organisations.[23]

2.4 IMPACT OF SANCTIONS

Sanctions Compliance and Over-Compliance Limit Users' Access to Key Services

As well as Iranian authorities' restrictive censorship measures, international service providers' compliance or over-compliance with US sanctions imposed on Iran have also resulted in many Iranians being denied access to a large part of the Internet, including a number of key online services.

In 2014, the US Office of Foreign Assets Control issued General License D1, which sought to reassure tech companies that they can make their services and

20 Khosro Kalbasi, Financial Tribune, 20/10/2019, "Iran Judiciary Moves to Ban Google Play", available at: **https://bit.ly/3pdN5Kk**

21 *Mehr News*, 03/10/2019, "Prosecution order to close download sites on web providers" [Persian], available at: **http://bit.ly/3jDRBAV**

22 *Khabar Online*, 9/10/2019, "Blocking movie download websites; removing competition for domestic sites?" [Persian], available at: **http://bit.ly/2NBe3i0**

23 *Fars News*, 28/02/2020, "Ban on the use of foreing messaging apps by government bodies, schools, and universities" [Persian], available at: **http://bit.ly/3s6tm1e**

content available to the Iranian public.[24] However, despite the fact that the US Treasury restated the content of GLD1 during the Trump administration, in recent years we witnessed a growing number of international service providers (including giant tech services) citing sanctions when limiting the availability of their services to Iranian users.

These decisions to close services to Iranians have had devastating short- and long-term effects on access to content and services. In the short-term, these policies have the same impacts as state-imposed censorship in Iran, and have resulted in the denial of users' connectivity to the global Internet. However, in the long term they have also pushed Iranian small- and medium-sized businesses to use alternative, Iranian state-backed domestic services, making it easier for the state to censor online expression, surveil users, and achieve its goal of localising the internet.

For example in January 2019 the American cloud infrastructure provider DigitalOcean emailed many of its Iranian clients stating that compliance with US sanctions would cause them to suspend their accounts within 72 hours. Deputy ICT Minister Amir Nazemi took to Twitter within hours to advertise Iranian domestic hosting services that had offered to host Iranian DigitalOcean clients free-of-charge for a 72-hour grace period in order to protect their businesses.[25]

24 *US Department of the Treasury,* "Sanctions Programs and Country Information", available at: **http://bit.ly/2Nuw1mo**

25 Kaveh Azarhoosh, *Filterwatch*, 11/07/2019, "Tech Giants Are Failing Iranians In Their Struggle Against A National Internet", available at: **http://bit.ly/3dqdjY0**

3 / STATE SURVEILLANCE

IRANIAN authorities have engaged in surveillance of users' activities online for many years. With the shift towards the localisation of the Internet in Iran, and the development of the National Information Network (NIN), the state's surveillance capacities are growing more sophisticated and more extensive by the month.

At the same time as the localisation of data is empowering state surveillance, Iran's judiciary and Cyber Police (FATA) have intensified their efforts to regulate and police online spaces, placing Iranians under further threat of monitoring and state sanction.

In this section, we catalogue the key developments in Iran's surveillance and monitoring capacities between March 2019 - March 2020: both in relation to policy development and the creation of new surveillance systems, and the expansion of online policing by FATA and other state security services.

3.1 POLICY DEVELOPMENTS

SCC Online ID Resolution Threatens Assault on Privacy Online

On 31 August 2019, the SCC passed a significant resolution which threatens an all-out attack on online privacy in Iran. The resolution is named the 'Valid Identity System in Cyberspace' resolution, and calls for the following:

- Every online interaction between different entities (to include individuals, parties, objects or services) must be conducted using a valid ID;
- Individuals will be identified using two sets of information managed by the ICT Ministry, known as an entity's "essential identity information" and their "attributes". The "essential identity" is one's fixed legal identity, whereas "attributes" are qualifications acquired by an entity over time.
- The National Centre for Cyberspace (NCC), working with the cooperation of the Executive and Judiciary should, within six months from the communication date of the resolution, draft the required regulations and legislation for establishing a Valid Identity System in Iranian cyberspace.
- The NCC should provide a report on the implementation of the resolution to the SCC every six months.

As part of the resolution, the ICT Ministry was asked to bring forward necessary new regulations and implementation plans, although these have not yet materialized.

The proposals outlined in this resolution would see the creation of enormous quantities of new, personally identifiable data about Iranian internet users, and their online activities. The requirement to associate online interactions with an "essential identity" comprising one's fixed legal identity could possibly see citizens' National IDs tied to all their activities online. The wording

of the resolution also suggests that "attributes" would be acquired by these identities over time; in theory, these could range from users' criminal records, to their education level, income, or health.

It is difficult to ascertain whether Iran genuinely seeks to implement a system of surveillance to monitor and record the interactions of all Internet users at all times. But the intentions expressed in this resolution serve as a serious warning to anyone concerned with digital rights in Iran.

The resolution that the expansion of state monitoring powers is a priority for the SCC. From reading the currently available text of the resolution, it is clear that authorities are working towards being able to more easily link the real identities of Iranian citizens with their online activities, a move that would make the implementation of a "layered filtering" system more feasible, and more likely.

3.2 SURVEILLANCE AND IAW ENFORCEMENT

FATA and the Policing of Online Spaces

Although there is no evidence to suggest that Iran operates a mass surveillance programme to monitor its citizens, the enforcement practices and public statements made by Iran's Cyber Police (FATA) nonetheless indicate the existence of active and far-reaching policing operations in online spaces.

Through public comments from FATA's top officials, we are able to understand how Iran's law enforcement and security forces engage in surveillance of Iranians' online activities.[26] Their actions, and the large-scale arrest of individuals based on their online activities also demonstrate that these surveillance measures are not being implemented solely for protection against exceptional national security threats, but to crack down on online expression – including political speech, but also other forms of expression that contravene state-sanctioned moral standards.

The rhetoric of FATA officials during this reporting period has tended to focus on their ongoing crackdown on "moral crimes"; largely focused on the online activities of women, as well as marginalised LGBTQ communities. FATA officials have also repeatedly discussed their operations to counteract internet users who they accuse of "spreading rumours and false information".[27]

The reach and power of FATA to police online spaces were particularly visible in relation to three major events: the protests and internet shutdown of November 2019, the shooting down of Ukraine International Airlines Flight 752 in January 2020, and the global

26 Kaveh Azarhoosh, *Filterwatch*, 18/02/2019, "Iran's Cyber Police — 'Society-Based Policing' and the Rise of Peer Surveillance", available at: **http://bit.ly/2Z042gL**

27 *Cyberpolice.ir*, 'Cyberspace users should be careful about spreading lies', 03/09/2019, available at: **https://bit.ly/3kF0lps**

COVID-19 pandemic commencing in Iran in February 2020.

In these incidents, FATA's oppressive policing of online spaces took on two different forms: firstly, the arrest and intimidation of high-profile users; and secondly, the mass arrest or intimidation of users with little or no public profile.

During this period we have repeatedly observed the arrest or intimidation of online personalities or known figures:

- Journalist Mohammad Mosaed was arrested for criticizing the government for the Internet shutdown during the November 2019 protests.
- Activist and women's rights campaigner Bahareh Hedayat was summoned to court after participating in and advertising protests in response to the downing of the Ukrainian International Airlines Flight 752 in January 2020.
- High-profile Instagram influencers such as 'Sahar Tabar' were arrested in October 2019 by FATA. She was charged with "disturbing public peace, encouraging immoral behaviour, and promoting violence". Later, IRIB broadcasted a confession video from her in which she expressed regret for her online activities.[28]

During this reporting period we also received reports of significant mass arrests coordinated by FATA, related to the ongoing COVID-19 pandemic. In April 2020, FATA announced that it had arrested 3,600 Iranians for "spreading rumours or false information" in relation to COVID-19.

FATA has also demonstrated that it seeks to use localized data in policing online spaces in Iran. On 26 May the CEO of Zanbil, an online shop in Iran, announced that access to the shop's payment system had been blocked.[29] This was as a result of the company declining to respond to a data request by FATA. Vakilzadeh told FATA that Zanbil would not comply unless presented with a formal written request.

Although the Iranian police and security forces have long monitored online spaces and taken punitive action against political dissidents and activists online (including the 2012 arrest and killing of blogger Sattar Beheshti[30]), this year saw a marked expansion of both the scope and capacity of their monitoring activities.

Today, state agencies are engaging in broad cultural and moral policing in online spaces, alongside their policing of political expression. These practices are designed to strike fear into users, and to encourage self-censorship

28 James Marchant, *Filterwatch*, 15/11/2019, "Filterwatch — October 2019", available at: **http://bit.ly/3p4Bz43**

29 *Peivast*, Twitter, 26/05/2019, available at: **https://bit.ly/3beiZSi**

30 *Reporters Without Borders*, 08/11/2012, "Jailed netizen Sattar Beheshti dies after prison interrogation", available at: **http://bit.ly/37hPcXA**

online. At the same time, the increased availability of locally hosted user data to further expand their capacities for monitoring citizens. These trends are of real concern, and point towards the continued erosion of online freedoms by police and security services in the years ahead.

4 / DIGITAL INCLUSION

ALTHOUGH there has been a huge increase in the number of people connected to the Internet since the Rouhani administration started investing in Iran's Internet infrastructure, significant inequalities still remain. Narrowing the digital divide in Iran, in particular connecting all rural areas to the Internet, was one of President Rouhani's campaign promises.

The ICT Ministry has formed public-private partnerships to attract investments to the project, and to expand the NIN's infrastructure around Iran. ICT Minister Mohammad Javad Azari Jahromi has repeatedly stated that these measures will not only bring the rural population online, but will also supply them with reliable and fast services. What this really entails is a 'censored-by-design' Internet for rural areas, and for other low-income segments of Iranian society that have no alternative infrastructure to turn to.

We should also note that ICT Minister Azari Jahromi has come under fire for the continued lack of connectivity in rural areas. On 17 June 2019 he attended a session of Iran's Parliament to respond to MPs' questions about the development of eGovernment services, and the government's plans for the development of internet infrastructure in rural communities. At the end of the meeting MPs were divided in their response – 83 MPs voted to express satisfaction with Azari Jahromi's answers, and 83 others voted to express their dissatisfaction. 7 abstained. As a result, Azari Jahromi received a formal warning from parliament.

While the digital gap persists, several policies, tools, and measures have recently been introduced that disproportionately affect vulnerable and marginalized groups such as women, religious minorities, low-income Iranians, Afghan students, and populations living outside of Iran's major urban centres.

This section elaborates on the most important highlights between March 2019 - March 2020, examining the impacts of Iranian ICT policy on an array of different marginalised groups. Taken together, this section will show how Iran's ICT policy apparatus is not only failing to close the digital divide, but is actively and purposefully excluding users from some of its most vulnerable and marginalised communities.

4.1 CHILD PROTECTION: TOWARDS A "CHILDREN'S INTERNET"?

Over the past decade, protecting children in cyberspace has been a high priority of Iran's ICT apparatus. In December 2014, Iran's Communications Regulatory Agency (CRA) banned the sale of SIM cards to individuals under the age of 18, and required mobile service providers to offer child-safe SIM cards within six months. Pursuant to this regulation, the Mobile Telecommunications Company of Iran (MCI, aka Hamrah-e-Aval) released the first SIM card for children to the market in April 2015. Shortly after, IranCell, the second major mobile

provider in Iran, followed suit and unveiled its children-only SIM card in May 2015.[31] More recently, other industry stakeholders have also taken appropriate measures. In its annual report, Cafe Bazaar reported that it released its first child-safe edition as part of its parental control initiative. The child-safe settings allow children to have access to age-appropriate games, content, and tools on Cafe Bazaar.

Over March 2019 - March 2020, a new policy push was geared toward expanding these efforts. In December 2019, the Deputy Director of Content Regulation at the National Center for Cyberspace (NCC) Amir Khorakian stated in an interview that his mandate includes regulating and monitoring digital content at large, including games and any content that impacts children and underaged individuals. A new NCC policy document titled 'Protection of Children and Teenagers in Cyberspace', which is under review by the Supreme Council of Cyberspace (SCC), advocates for two measures: (1) dedicated technical infrastructure for a children's Internet, and (2) encouraging the mass production of age-appropriate digital content to circulate on the so-called "children's Internet."[32] It remains unclear what an age-appropriate Internet will entail technically. From Khorakian's remarks, it can be surmised that a completely independent technical layer may not be required. But the NCC may assign the ICT Ministry to consider and dedicate resources to child protection mechanisms on the Internet.

This was not the first time that the idea of a children's Internet has been raised by Iranian authorities. The concept has been floating around since ICT Minister Azari Jahromi launched a campaign for child protection on the Internet in 2017. Since then, the ICT Ministry has released draft documents on a national plan for protecting children in cyberspace. These documents have put forward several recommendations, including expanded parental control mechanisms and clearer responsibilities on the part of ISPs to protect minors. The documents also promote multiple home-brewed parental control programs such as Anarestan,[33] Donya-ye-Dorsa, Sunyar, and Shaghayegh.[34] The first two programs are branded as "digital ecosystems" for protecting children on the Internet. In reality, these are state-sanctioned vendors that offer child-safe SIM cards and pre-installed services, such as a child-safe app store, application software, and other tools. The recent NCC plan seems to be a non-binding policy plan to formalize and

31 *Digiato*, 13/05/2015, "Irancell Launched the first phase of its Children and Adolescents' Service" [Persian], available at: **http://bit.ly/2N3C3KE**

32 *ISNA*, 24/12/2019, "Separation of public internet and children's internet" [Persian], available at: **http://bit.ly/3qmir30**

33 *MCI*, "Student SIM Cards" [Persian], available at: **https://mci.ir/student-sim-cards**

34 *Iranian ICT Ministry,* "Draft Plan for Protecting Children in Cyberspace" [Persian], available at: **https://bit.ly/2N9CEKR**

facilitate the implementation of what the ICT Ministry had already started.[35]

4.2 WOMEN'S EXPERIENCES: INSTAGRAM & COMPULSORY HIJAB

In May 2020, Iran's Cyber Police (FATA) announced that removing headscarves on virtual platforms will carry the same consequences as in public places.[36] Under Iran's Criminal Code, removing compulsory hijab in public is a punishable offense, which can result in sentences of 10 to 60 days in prison and/or a fine. However, the announcement cited the Cyber Crimes Law's clauses on "disseminating indecent content" as the legal ground for this new rule.[37] The law will reportedly apply to Instagram influencers and ordinary users alike, regardless of the reach of their content. While enforcement will be a challenge, Iran has repeatedly demonstrated willingness to limit access to content that contravenes state-defined interpretations of Islamic values (particularly where they affect women and their bodies).

Previously, in 2014, Iran pursued a $2.6 million "smart filtering" project that attempted to selectively block parts of "inappropriate content" without blocking an entire page or domain.[38] Due to its popularity among Iranians, Instagram was the main target of this smart filtering initiative. However, the project was abandoned after Instagram applied SSL encryption as standard. In November 2019, the SCC moved to revive parts of the smart filtering project with a new proposal to pursue "layered filtering" of Internet content according to a individual "needs." Again, the enforcement of such policy can be cumbersome. Nonetheless, it underscores Iran's ambition to create customized experiences for Internet users, subjecting them to increasing scrutiny and undermining net neutrality.

4.3 RELIGIOUS MINORITIES: BAHA'IS FACE EXCLUSION FROM NEW E-GOVERNMENT INITIATIVES

The Baha'is of Iran have suffered a long history of persecution, tragedy and trauma. Exclusionary policies, coupled with broader societal prejudices against the Iranian Baha'is have severely impacted their access to higher education, economic prosperity, and even digital communities. Since the early days of the 1979 Islamic Revolution, Baha'is have been barred from pursuing higher education. Unless they conceal their religion, which goes

35 *Mehr News*, 6/12/2020, "Plan for child protection in cyberspace awaiting approval" [Persian], available at: **http://bit.ly/2M1gnOS**

36 *DW Farsi,* 19/05/2020, "Iranian Police: Hijab is mandatory in Iran, even on Instagram" [Persian], available at: **http://bit.ly/3deEogK**

37 *Article 19,* 22/05/2020, "Cyber Police warning to women without hijab online, another attack on women's freedom of expression in Iran" [Persian], available at: **http://bit.ly/2MYwkpJ**

38 *ISNA*, 07/09/2019, "How much did smart filtering cost?" [Persian], available at: **http://bit.ly/3u0g8ET**

against their religious beliefs, Baha'is students are not allowed to register at higher education institutions. Online Baha'i content is also largely blocked.

Moreover, their online presence is barely tolerated. Their digital communities on Facebook are infiltrated and targeted with threats and intimidating messages. Baha'i businesses are often attacked and vandalized, adversely affecting their livelihoods. In May 2019, Iran's Supreme Leader issued a fatwa that banned Muslims from having any financial interaction with Baha'is.[39] Furthermore, the Baha'is are frequent targets of inflammatory and baseless accusations by the state media and Iranian officials, presenting a distorted image of the Baha'is to the Iranian public. Over the past year, Iran has adopted new policies that exacerbate the persecution of the Baha'is in unprecedented ways.

Starting in January 2020, the Civil Registration Organization (CRO) of Iran adopted a new policy to issue smart ID cards. Pressured by several conservative MPs, the CRO changed the wording of the ID card application to reflect a discriminatory policy against several religious minorities, in particular the Baha'is.[40] To qualify for the new card, applicants must be followers of Islam or one of the other religions recognised under the Iranian Constitution. This means excluding other religions that are not formally acknowledged by the Constitution, most notably the Baha'is.[41]

The policy has significant implications as it affects the ability of card holders to seek any of Iran's e-government services. These services span from financial transactions and online banking to applying for passports and criminal record checks (required for some job applications). Excluding the Baha'is from the e-government ecosystem violates their economic rights, livelihoods, and access to equal civil, social, and economic opportunities.[42]

39 *Khabar Online,* 02/05/2019, "Leadership fatwa: sharia rules on associating and dealing with Baha'is" [Persian], available at: **http://bit.ly/3b9ypXI**

40 *Campaign for Human Rights in Iran,* 27/01/2020, "Iran has denied the possibility of granting unrecognised religious minorities National ID cards", available at: **http://bit.ly/2NuvCAo**

41 *Iranwire*, 23/01/2020, "Baha'i citizens deprived of national ID cards; is there a way to object?" [Persian], available at: **https://bit.ly/3k2JFcI**

42 Other resources: BBC Persian, 27/01/2020, "Concerns from the international community over new restrictions on smart ID cards in Iran" [Persian], available at: **http://bbc.in/2NGe3x3**, Deutsche Welle, 24/01/2020, "Baha'is will have to lie or forget national ID cards" [Persian], available at: h**ttp://bit.ly/3s02fEM**, Radio Farda, 23/01/2020, "Baha'i citizens in Iran are facing issues in getting national ID cards" [Persian], available at: **http://bit.ly/3pyurwU** and Iranwire, 29/12/2019, "Smart national ID cards will not be given to Baha's citizens in Iran", available at: **https://bit.ly/3k2UOKc**

4.4 ONLINE EDUCATION SERVICES AND MARGINALIZED STUDENTS[43]

For the past two decades, Iran has been entertaining ideas for establishing an ecosystem of virtual education. In 2003, the Ministry of Education was authorized by the Supreme Council of Cultural Revolution to pursue in-person, hybrid, and remote methods of education. In the face of COVID-19 and the closing of schools in many parts of the country, the Ministry of Education was pushed to move classrooms online via a domestically developed application, Educational Network of Students (Shaad). The network was launched a few weeks after the Nowruz holidays to facilitate the return of students to a regular schedule.[44] Shaad offers web, Android, and iOS applications. To create an account, one needs an Iranian mobile number (country code +98) and to provide a national identification number.

According to government data, by April 28 the Shaad application had been downloaded about 12 million times, with over 8 million students and almost 625,000 teachers signing up to the platform, and more than 18 million files exchanged.[45] However, the application's performance has not been satisfactory. In addition to recurring crashes, it has been extremely slow for real-time education. Teachers were not able to upload classroom materials prior to classes, students were unable to submit questions during the classes, and other message exchanges did not go through. The state's insistence on the localisation of platforms – without securing their technical foundations – has undermined the efficacy of Iran's educational system during this crisis.

Moreover, the new network has underscored several issues pertaining to educational justice. First, the identification requirement originally excluded non-Iran-born students, the majority of whom are of Afghan origin. These students often do not own Iranian birth certificates or national identity cards – a situation that bars them from access to education and public health systems. In addition to Afghan students, Shaad could exclude Baha'i students too. As we explained in the previous section, Baha'is do not qualify for the latest national identification cards. This can mean that Baha'i students who do not receive a new ID card will not be able to use the Shaad application. While the Minister of Education announced in late April that Afghan students could sign up to Shaad with their registration number for foreign citizens, no solution has been proposed for religious minorities who

43 *Iran Moshavere*, "Entering the Education Ministry's Shaad system" [Persian], available at: http://bit.ly/3atGUxN and Majazist, 24/06/2020, "Startups collaborate with Shaad" [Persian], available at: **http://bit.ly/3s6wMRv**

44 *Iran Moshavere*, "Entering the Education Ministry's Shaad system" [Persian], available at: **http://bit.ly/3atGUxN**

45 *Dolat.ir*, 21/04/2020,"Latest statistics on Shaad education users" [Persian], available at: **http://bit.ly/3bcmk3U**

may be deprived of an identification number.

Second, by relying on online communication, the new method disproportionately excludes students in remote areas. Due to the lack of reliable infrastructure in non-central areas, many households do not have access to landlines or mobile networks, which by default excludes students from these regions from connecting to Shaad. Iranian authorities claim that alternative methods of access to educational content have been provided to ensure that the policy is implemented inclusively. Alternatives include offering in-person classes at a much lower capacity, distributing educational content via paper copies, and other digital formats (for example on CD and DVDs).[46] Regardless, one report from June 2020 noted that 47% of students in Kohgiluyeh and Boyerahmad province were estimated to have not been connected to Shaad, illustrating the potential scale of these disparities in rural areas.[47]

Third, the smartphone requirement further marginalizes many students. Low-income households are unable to provide their children with dedicated smartphone devices. In the medium-income stratum, the number of smartphones per family may be limited, which hinders simultaneous access to Shaad for more than one student at a time. Even in households where financial considerations are less restrictive, lack of parental control over the children's use of smartphones during business hours has become a concern.

These challenges have revived discussions about the important role that the IRIB can play in providing unilateral access to educational material. Proponents argue that given the extended penetration rate of television, IRIB could facilitate the distribution of educational content to remote areas to remedy the lack of access to the Internet and smartphones. While access to television is not guaranteed in these regions, the idea has received traction particularly among conservative officials and media outlets. Overall, however, Shaad has raised more concerns than solutions to the challenge of education in a country that is hard hit by the COVID-19 pandemic.

4.5 BORDER PROVINCES: EXTENDED SHUTDOWNS IN SISTAN & BALUCHESTAN

The 2019 internet shutdown ended after about a week in most parts of Iran.[48] However, areas outside of Iran's urban centres and the country's border provinces took much longer to restore

46 *IRNA*, 29/04/2020, "Shaad network; innovation in education with a hazy future" [Persian], available at: **http://bit.ly/3s0HFEz**

47 *Majazist*, 25/06/202, "47% of Students in Kohgiluyeh and Boyerahmad are not connected to Shaad" [Persian], available at: **https://bit.ly/2Z9ogEy**

48 Small Media, *Filterwatch*,19/11/2019, "Iran Shutdown Monitor", available at: **http://bit.ly/3tDdx3L**

access to the Internet. In particular, Sistan and Baluchestan province lacked Internet access – landline or mobile – for more than 18 days. The Internet shutdown was prolonged due to security concerns over the arrest of an influential Imam from the region, who supported the uprising in opposition to the fuel price hike.

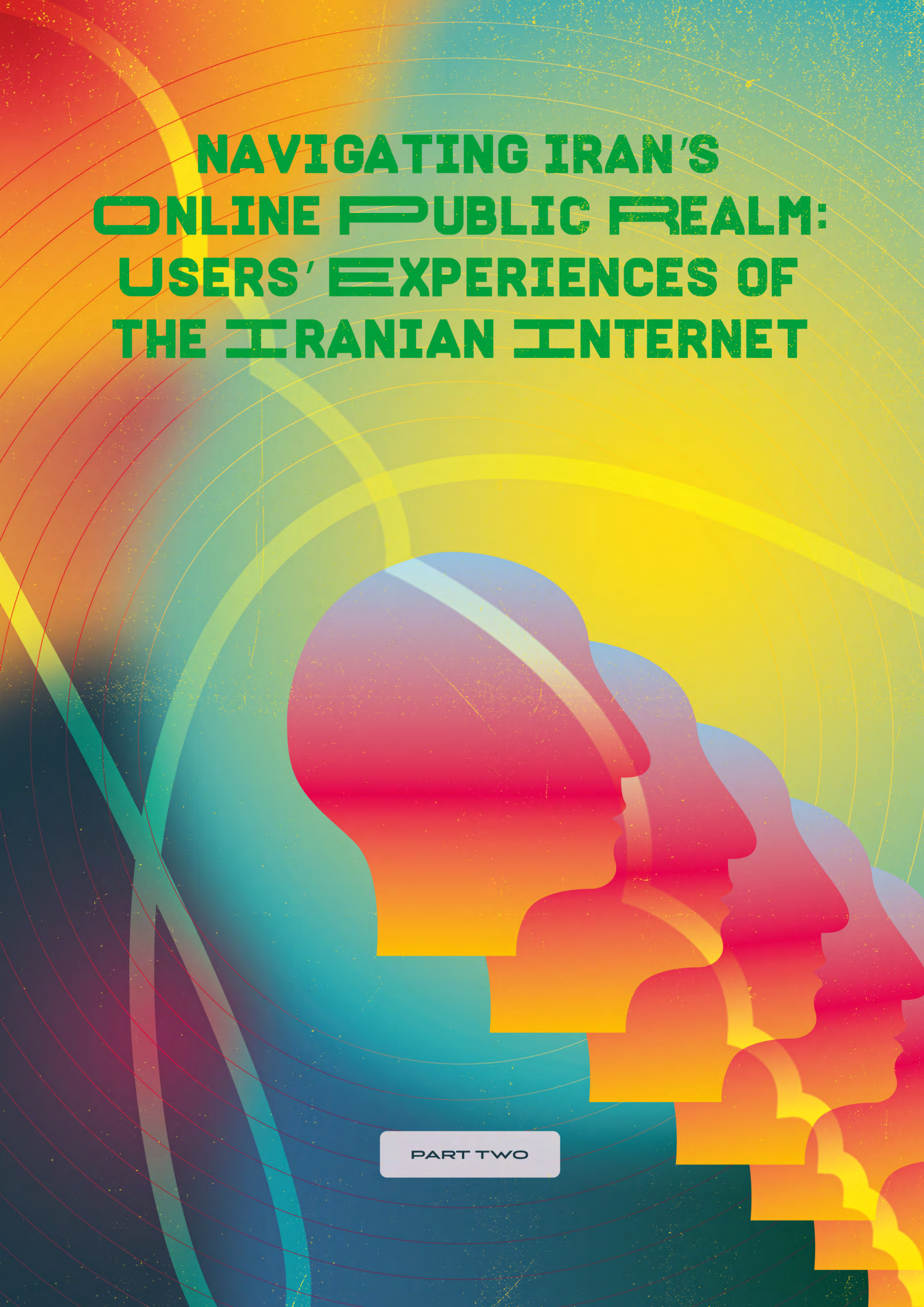
The government response saw a large deployment of security forces across the region and a prolonged Internet shutdown that disproportionately affected local businesses and entrepreneurs.[49] The situation also put strains upon a trade agreement between Iran and Pakistan to bolster cross-border cooperation.[50] Sistan and Baluchestan is Iran's least connected province, with 2.94% landline and 57.4% mobile broadband penetration rates.

In addition to the particular situation in Sistan and Baluchestan, anecdotal reports indicate that other areas outside of Iran's major centres faced heavy-handed surveillance and suppression of protests, and were also slow to come back online. In this sense, these already marginalised and economically left-behind regions of Iran were those that bore the highest economic and social costs of the shutdown.

49 *Hamshahri News*, 06/12/2019, "Vaezi's comments on the internet shutdown in Sistan and Baluchestan" [Persian], available at: **http://bit.ly/3s0a39x**

50 *DW Farsi*, 04/12/2019, "Internet shutdown in Sistan and Baluchestan has made life on either side of the border difficult" [Persian], available at: **http://bit.ly/3jOYb7L**

NAVIGATING IRAN'S ONLINE PUBLIC REALM: USERS' EXPERIENCES OF THE IRANIAN INTERNET



PART TWO

PART II

NAVIGATING IRAN'S ONLINE PUBLIC REALM: USERS' EXPERIENCES OF THE IRANIAN INTERNET

THE policy developments discussed in the previous chapter have been responsible for altering the nature of online spaces in Iran, and the experiences of Iranian internet users. In many cases, these policies have made the digital public realm less secure, less open, and more vulnerable to the spread of misinformation.

The following chapters present a picture of Iranians' experiences of navigating these spaces; they explore the consequences of data insecurity, issues of online disinformation and closed media spaces, and Iran's increasingly localised and inward-looking ICT sector.

5 / DATA SECURITY

WITH the rapid growth of the domestic digital economy, online services, and general internet usage it is inevitable that Iranians will find themselves exposed to an increased number of data leaks and insecurities. However during the year under review Iranians experienced a particularly high number of data leaks, including a devastating incident relating to the messaging app Telegram which exposed sensitive data from the equivalent of nearly half of Iran's population to open trading online.

The localisation of the internet, twinned with a lack of any substantive legal data protection framework in Iran has created an unsafe online environment where the sensitive data of Iranian users routinely finds its way into the public realm.

5.1 MAJOR DATA LEAKS

In the year covered by this report, Iranian internet users experienced a number of major online security breaches, with millions of items of data leaking from communications apps, banking services, and popular transport apps. The frequency of these incidents speaks to Iran's failure to craft any adequate data protection laws, and its inability to ensure that Iranians' data remains secure and private.

Here are some of the worst examples of data breaches from this year:

42 Million Telegram Records Leak, 'Forked' Apps to Blame

In late March, Comparitech and Security Researcher Bob Diachenko revealed that 42 million records from Telegram used in Iran had been leaked online.[51] The data is said to have been posted by a group called "Hunting System" on an Elasticsearch cluster which did not require a password or authentication in order to access it. According to Telegram, the data was taken from third-party or 'forked' versions of the app which are built using Telegram's open source code. The exposed data included user account IDs, usernames, phone numbers, hashes and secret keys. The leaked data compromises the security of users, placing them at the risk of a number of harms such as SIM swap attacks. The data was eventually removed after it was reported to the hosting provider.

'Forked' versions of Telegram gained popularity among users inside Iran as a way of accessing the app following the filtering of Telegram in 2018. These apps lack security features, are insecure, and put their users at risk. Two popular clone apps "Hotgram" and "Golden Telegram" were developed by "Smart Land Strategy" a company said to be connected to Iran's intelligence forces. The apps were eventually removed from the Google Play Store due to spyware and malware concerns. Their servers inside the country were eventually turned off, and the apps went offline.

51 Melody Kazemi, *Filterwatch*, 23/04/2020, "Policy Monitor — March 2020", available at: **http://bit.ly/37jrfPz**

15 Million Bank Accounts Breached
Just a month after the violent protests and and the Internet shutdown of November 2019, 15 million debit card numbers from some of Iran's major banks were published[52] on social media, equivalent to nearly a fifth of Iran's population. ICT Minister Azari Jahromi blamed the breach on a rogue contractor who had published the data in an extortion attempt rather than on a hacking attempt. This claim was disputed by security experts, who perceived the breach as the work of a state entity.

Driver Data for Ride Hailing App Tap30
Highly sensitive, personally identifiable information of thousands of drivers for the Iranian ride hailing app, Tap30 were discovered publicly available online in April 2019 by Security Researcher Bob Diachenko.[53] Iran's Cyber Police, FATA, confirmed[54] that Tap30's servers lacked adequate security measures.

The data leaks and security breaches highlighted here - which are becoming increasingly common each year - underscore the lack of attention and prioritisation of adequate security measures by a number of Iranian technology companies. Alongside a legal data protection vacuum, data from Iranian internet users are under constant threat not just from malicious actors, but also from data misuse by developers as well as by the state as means for enhanced surveillance. The practices of internet localisation, which increasingly restrict online freedoms, have forced citizens to compromise their safety and security in order to find ways to gain access to the global Internet.

So far, the Data Protection Bill proposed in 2018 has not yet made its way to Majles for the consideration. This bill, which was proposed by Jahromi's ICT Ministry in collaboration with the Judiciary, answers some of the needs for data protection in Iran, However, it still priotises surveillance and data localisation over privacy and data security of the users in Iran, making the project wholly incompatible with international data protection standards.[55]

52 Farnaz Fassihi and Ronen Bergman, *New York Times,* 10/12/2019, Iran Banks Burned, Then Customer Accounts Were Exposed Online", available at: **http://nyti.ms/3rPUXU6**

53 Bob Diachenko, *Security and Discovery,* 18/04/2019, "Iranian Ride-Hailing App Database Exposure", Available at: **http://bit.ly/3rSEGOn**

54 *Tabnak Javan*, 29/04/2019, "How was the data for TAP30 drivers leaked?" [Persian], Available at: **http://bit.ly/3b1oBik**

55 Melody Kazemi, *Filterwatch*, 19/06/2020, "Data Insecurity On Iran's Localised Internet" [Persian], Available at: **http://bit.ly/2H80a7J**

6 / PATTERNS OF INFORMATION CONSUMPTION

As the Internet penetration rate increases across Iran, new audiences are coming online. These new users are entering an online world that differs dramatically from the one that existed even a few years ago. As a result, their patterns of online media consumption and application usage are evolving from those of previous internet users.

Why is this? For starters, the expansion of entrepreneurial initiatives in Iran has influenced the ways that netizens understand and seek to take full advantage of all that the Internet has to offer, despite all the technical and political challenges that exist. This section of the report turns to patterns of information consumption in society, state interventions in manipulating public opinion, and civil initiatives to address information contamination.

The section progresses in two parts. First, we review consumer trends from Cafe Bazaar, the largest domestic Android app store in Iran, for a bird's eye view of the tools and platforms that Iranians used over the course of 2019-2020.

Then, we elaborate on the expansive issue of information disorder, from misinformation and disinformation, to targeted harassment and the conspiracy theories that increasingly contaminate digital public spaces. As we note, the state has a particular interest in manipulating public information on a range of issues, including matters relating to national security and Islamic values. The section closes by discussing a handful of civil initiatives that have sought to address information disorder, educate the Iranian public on the matter, and to increase web literacy in society.

6.1 CONSUMER TRENDS & CAFE BAZAAR

To better understand domestic consumer trends, we focus on the usage of digital tools as reported by domestic platforms. In particular, we refer to the Cafe Bazaar data for two reasons. First, although Iranians heavily rely on international platforms to connect to the Internet, reliable information about the usage of international platforms by Iran-based audiences is scarce. When such information is indeed available (e.g. Google Trends), it is often obfuscated by the use of VPNs and proxy tools that enable Iranians to bypass the state-imposed censorship. Therefore, exploring data from Iran-based companies offers a direct window into consumer behavior in Iran.

Secondly, Cafe Bazaar is the largest home-grown Android app store in Iran, offering services similar to those of Google Play's. Over the past decade, Cafe Bazaar has acted as a bridge between consumers and app developers, enabling access to the latest technologies for many Iranians. It is also largely consistent in its reporting: Cafe Bazaar has released quarterly and annual reports for the past three years. The following section is based on Cafe Bazaar's annual report for the

final quarter of 1398 (March 22, 2019 - March 21, 2020).

By the end of the last Persian calendar year, Cafe Bazaar had 41 million active installations, with 1.85 billion downloads and updates of games and applications. Cafe Bazaar reported that 3.7 million clients purchased digital tools and services, and that 24 million transactions were successfully processed over the past year. As a result, app developers generated about 4.5 million USD in net revenue -- a figure that indicates an 84% increase compared to the previous year. These figures are promising despite the setback that most online businesses experienced by the COVID-19 pandemic that hit Iran especially hard in February 2020.

In the first quarter of 1398, "Telegram", "Golden Telegram", and "Games" were the most searched for keywords on Cafe Bazaar. Golden Telegram is a domestic, unfiltered version of Telegram that is suspected of having ties with Iran's intelligence services and being used for surveillance purposes. In December 2018 Telegram specifically targeted its users against Iran's domestic 'forked' versions of their open-source application, raising concerns over the use of this seemingly innocuous duplicate.[56] Responding to repeated requests from internet freedom advocates, on 25 April 2019 Google Play took down all forked versions of Telegram that were accused of spying on Iranians, and which were suspected of having connections with the Iranian government.[57]

With these forked, and unblocked, versions of the popular messaging app Telegram off the market (and their servers later shut down by developers in June 2019),[58] users began their search for alternatives. This perhaps explains the shift in the most-searched keywords, starting in the second quarter of the past year. According to Cafe Bazaar, for the rest of the year, most keyword searches included "Games", "Instagram", and "WhatsApp" (with the exception of July 2019, which still shows traces of searches for the original version of Telegram).

Out of 109,000 applications that were offered on Cafe Bazaar over the past year, the categories of 'Education', 'Religion', and 'Books' comprised the largest categories of apps. Educational apps alone comprised 23% of applications. Digital tools comprised only 4% of all programs but were downloaded and updated more than any other categories, followed by 'Practical Tools', 'Messaging' (1% of programs),

56 *ICHRI*, Twitter, 15/12/2018, **https://bit.ly/3jYEp9W**

57 *BBC Persian*, 25/04/2018, "Golden Telegram and Hotgram Removed From Google Play For Espionage" [Persian], available at: **http://bbc.in/3dsRabF**

58 *Digiato*, 22/06/2019, "The End of Golden Telegram and Hotgram; Servers Shut Down" [Persian], available at: **http://bit.ly/3ipLXl5**
Other resources: Digikala report of the first half of 1398 [Persian], available at: **http://bit.ly/2NlYta9** and Virgool's annual report for 1398 (March 2019 to March 2020) [Persian], available at: **https://bit.ly/3axUn7L**

and 'Educational Apps' (23% of total applications).

By the end of the year, 18,000 games were available on Cafe Bazaar. They were downloaded and updated over 670 million times, indicating a highly popular trend among Iranian users. Notably, games generated a third of the total revenue on the app store. educational games received the largest number of active installations.

The highest rated categories of apps were respectively 'Sports', 'Religion', and 'Finance'. Applications related to 'Finance', 'Music', 'Sound', and 'Social Media' had the largest growth rate, compared to the previous year.

With 20 million downloads, the app Divar (a domestic online market for goods and services similar to eBay) topped the annual downloads. Notably, the domestic messenger Soroush (which has generated much controversy since the blocking of Telegram) had 2 million new downloads over the past year (see **Case Study 1**).

Notably, in the face of the COVID-19 pandemic, Cafe Bazaar actively promoted applications that would reduce unnecessary travel or commuting, such as telemedicine and banking services, remote work and productivity tools, and online shopping platforms.

6.2 MISINFORMATION & DISINFORMATION

Iran views itself as being embroiled in a soft war with its adversaries abroad, one of which is the Western media. In response, Iran has waged domestic and international influence operations to claim authority over the information space, shift media narratives to its own interest, and correct distorted images of the Islamic Republic in the eyes of domestic and international audiences. To this end, the Islamic Republic has sustained an army of pro-regime media outlets that frequently bolster Iran's rhetoric. These platforms also shape political, social, and cultural narratives by producing inaccurate news, tweaking reality, and smearing specific communities and individuals. These narratives and measures often correspond with Iran's dominant social and political contours.

In addition to conservative news outlets, Iran has fostered an unofficial army of hawkish social media activists who propagate the state's rhetoric on different platforms, including on Twitter and Instagram. These communities create and promote campaigns, conveying loyalty to the hardliners, the Supreme Leader of Iran, and the IRGC, to name a few. They often behave in a coordinated manner, using offensive language and messaging to suppress dissidents and activists on virtual platforms like Instagram. Through inauthentic behavior, they seek to dominate the information space, undermine the public's trust in influential figures, and also manipulate public opinion on matters of strategic interest to the Islamic Republic.

CASE STUDY 1. THE BLOCKING OF TELEGRAM: TWO YEARS ON

Two years after the filtering of Telegram went into effect, it's still one of the most popular messaging applications among Iranians, a new infographic by the reformist news portal Etemaad Online shows.[59]

According to this infographic, by the end of March 2020 over 42% of Iranians (about 30 million) used Telegram. This information is consistent with prior polling results by Iranian Students Polling Agency (ISPA). In July 2019, ISPA indicated a migration trend from Telegram to WhatsApps among Iranian users, making Telegram the second popular messaging application. According to the ISPA poll, 42.8% use WhatsApp, followed by Telegram (42.4%), and Instagram (39.5%). [60]

Etemaad Online also reports that during the country-wide quarantine due to COVID-19, Iranian students and teachers heavily relied on Telegram to exchange educational content. Since 2013, Telegram has remained a critical source of information to Iranians during other crises, including the IRGC's shooting down of the Ukrainian International Airlines Flight 752 earlier this year, and the November 2019 protests.

The State of Soroush: Etemaad Online estimates that fewer than 8 million Iranians use the top 5 domestic messaging applications, including Soroush and iGap. The ISPA poll shows that only 2.8% use the home-brewed messaging application, Soroush, which has been heavily subsidized by Islamic Republic of Iran Broadcasting (IRIB).

In early March 2020, IRIB announced that it was accepting bids for Soroush from the private sector. The latest announcement suggests an opening price of about $1 million for Soroush.[61] The company has reportedly received

59 Etemaad Online, 01/05/2020, "Two Years After the Filtering of Telegram" [Persian], available at: **https://bit.ly/3qFSYkX**

60 ISPA, 21/07/2019, "Migration From Telegram to WhatsApp" [Persian], available at: **http://bit.ly/3pvYHc5**

61 *Peivast*, 10/03/2020, "Behind the Scenes of the Soroush Messenger Auction" [Persian], available at: **https://peivast.com/p/72229**

$120,000 in state-subsidized loans.[62] IRIB officials claim that Soroush has matured as an entrepreneurial project and is ready to sustain itself in the market.[63] Others, including Iranian media and Twitter users, consider Soroush an utter investment failure for IRIB -- one that promised to compete with Telegram but failed completely.

On the Filtering of Telegram: Telegram was blocked on 30 April 2018, after an order by Iran's Judiciary. At the time of blocking, Telegram was estimated to have 40 million users in Iran. In response, Iranian users rushed to apply circumvention tools to stay connected to Telegram despite the concerted efforts of different political bodies to diminish attention to the app. Much of the state's effort centered on migrating Telegram users to domestically developed alternatives such as Soroush and iGap. However, users expressed serious concerns about the security of state-sanctioned applications, and considered them to be facilitating state surveillance.

Why Telegram is so controversial: The political contention over Telegram dates back to 2016 when reformists leveraged the messaging application in a parliamentary election to transform the way political campaigns were run. As a result, reformists won the majority of parliamentary seats against conservatives. Similarly, Telegram played a key role in 2017 during the presidential election, which led to the re-election of the moderate president Hassan Rouhani. Later, during Iran's 2017-18 unrest, popular Telegram channels like Amad News were sites of both anti-government criticism and coordination of protests, and officials subsequently criticised Telegram for "encouraging hateful content.".[64]

62 *ISNA*, 10/03/2020, "Advertising the Sale of Soroush. Who's buying?" [Persian], available at: **https://bit.ly/3oSqxiR**

63 *Tejarat News*, 06/04/2020, "Why is Soroush Messenger Being Put Up For Auction?" [Persian], available at: **http://bit.ly/38RGiB7**

64 Farangis Najibullah, 05/01/2018, "Controversial Exile Using Social Media To Try To Bring Down Iranian Government", available at: **http://bit.ly/2ZhFPCX**

Research has shown that these communities tend to follow similar accounts, target similar communities (including LGBTQ activists, journalists, outspoken diaspora dissidents, and celebrities), and promote content that signals their religious and political affiliations.[65]

Moreover, the strategy of outsourcing censorship and media manipulation has reached Wikipedia.[66] In recent years, the Ministry of Culture and Islamic Guidance has bolstered support for managers and editors of Persian Wikipedia, hosted their summits at the Ministry, and put forward a proposal to formalize a public-private partnership as a non-governmental organization, hosted at the Ministry.[67] This media strategy seeks to fill in the gap with state-sanctioned information about issues of strategic interest to Iran, including its involvement in the Syrian war, regional allies like Bashar Assad, and the nuclear program. Having established themselves as a 'legitimate' editorial team, Persian Wikipedia editors also seem to monitor the information that goes into the Wikipedia pages of high ranking Iranian officials. They have gained enough authority to remove any information that challenges the official rhetoric of the Islamic Republic, censoring the largest public encyclopedia for the Persian-speaking audience.

In the past year, Iran's media manipulation apparatus has sought to dominate the digital media with state-sanctioned narratives, presenting a distorted image of reality and leveraging these platforms to their own advantage. These operators took an active role in many occasions over the past year. Examples include Iran's involvement in anti-US protests in Iraq (December 2019), the killing of Qassem Soleiman, the former leader of the IRGC's external branch of Quds Force, in a US drone attack (January 2020), and the downing of Ukraine International Airlines Flight 752 due to an error of IRGC operators (January 2020).

In addition, the COVID-19 pandemic offered a renewed opportunity for persecution[68] of the Baha'is in the form of disinformation. In March 2020, the hardliner Kayhan News[69] (close to the Supreme Leader of Iran) and other

65 Simin Kargar, Adrian Rauchfleisch, 24/01/2019, "State-aligned trolling in Iran and the double-edged affordances of Instagram" *New Media & Society,* available at: **http://bit.ly/3qnx46f**

66 Sina Zekavat, 11/09/2019, Open Democracy, "Persian Wikipedia: an independent source or a tool of the Iranian state?", available at: **http://bit.ly/35NLIuZ**

67 Ministry of Culture and Islamic Guidance (Media), 16/09/2018, "Audio and Visual Report of Meeting on Wikipedia Techniques in Information" [Persian], available at: **http://bit.ly/35Koeql**

68 *Factnameh*, 13/03/2020, "Accusations of Organised Hoarding By Baha'is By a Member of Parliament" [Persian], available at: **http://bit.ly/3jNKfLa**

69 Kayhan News, 03/03/2020, "The Bahai Sect Are Happy With the Spread of Corona in Iran, and Do Business With the Health of the People" [Persian], available at: **https://bit.ly/3jShGw6**

conservative news sites[70] accused the "Baha'is" foreign-based media, such as BBC Persian, Manoto, Iran International, of being 'joyful' about the pandemic hitting Iran so hard. Over the past decade, the Islamic Republic and its media cycle have demonized the Baha'is and liberally used the term for othering dissidents, diaspora journalists, and activists. In this recent case, the term 'Baha'is' is used in a derogatory sense to refer to the foreign-based alternative media that sought to cover the scope of the pandemic in Iran, the government's lack of efficient response, and its efforts to suppress the free flow of information about the pandemic. These allegations were amplified by accusations from one member of parliament, who alleged that the Baha'is businesses were stockpiling masks while the country needed them most.

In the long run, these practices enable the government to move away from traditional censorship and adopt more nuanced, post-constructivist approaches to media manipulation instead. Since 2018, Twitter and Facebook have taken the initiative to remove state-affiliated assets in influence operations that target international audiences. Most industry research is based on these internationally-oriented datasets. However, limited research has been conducted on the nature and scope of domestic influence operations, that can often give important context to international campaigns.

There are some hopeful signs for Iran's media ecology, however. In recent years, Iranian Internet users have become more savvy to detect politically oriented campaigns and accounts. As with other societies, there is still a long way to go against false information and disinformation. It is in this context that civil society initiatives like the fact-checking website FactNameh[71] can play an important role in debunking such claims. Over the past year, other civil society initiatives such as Digital Shahrvand[72] have sought to educate the public on such coordinated inauthentic behavior, debunk some of the misinformation and disinformation that go viral on social media platforms, and engage the public for further debate on these issues.

The development of media literacy and building public resilience to misinformation campaigns is not a challenge unique to Iran. In Iran, as globally, this is an effort that will require a sustained effort from journalists and civil society. But the growth of such initiatives over the past year offers some hope that a healthier information environment is possible.

70 *Afkar News*, 03/03/202, "The Bahai Sect Are Happy With the Spread of Corona in Iran" [Persian], available at: **https://bit.ly/2XKXVgC**

71 *Factnameh*, Website, available at: **https://factnameh.com**

72 *Digital Shahrvand*, Website, available at: **https://digitalshahrvand.com/**

7 / MEDIA PLURALITY

ONE of the goals of Iran's localisation and information control agenda in recent years has been the weakening of media plurality in online spaces. Iran has had a rich history of citizen media and journalism in the past two decades. Arguably the foundation for online activism and dissent was laid in Iran in the early 2000s when Iran had a disproportionate number of young bloggers. Over the last decade, online platforms and messaging apps have given birth to new forms and generations of citizen media.

Over the decade we have also witnessed new waves of diasporic Persian language media with significant popularity in Iran. This is one of the central reasons that the localisation of online media consumption, and the suffocation of media plurality has been at the center of Iran's new information control policies and practices. In this section of the report we take a look at how these policies and practices shaped online media plurality in Iran during the year 1398.

7.1
THE GROWING ROLE OF INSTAGRAM

Filterwatch's September 2018 report highlighted the massive popularity of Instagram among Iranians.[73] To its more than 26 million active users – amounting to 32% of all Internet users in Iran – it is first-and-foremost a place to share and view user-produced images and videos. It has also prompted a surge in user-based content in a way that no other platform or app has, owing to its legal availability and straightforward accessibility to anyone with a smartphone.

Its position as the "last platform standing" has meant that a diverse set of communities have been utilizing Instagram in innovative ways. Marginalised communities such as religious minority communities, LGBTQ, and cultural and linguistic minorities have used the platform to share resources, and to form short- and long-term communities online. In addition, politicians have been actively using Instagram to connect with voters, constituents, and the general public. In 2017, Instagram was a key platform for presidential campaigns, with reformists and conservatives equally using Instagram Live to directly communicate with voters.[74] During the COVID-19 pandemic, Instagram Live became the nexus of public discourse outside the mainstream media and state-controlled channels.

73 Kaveh Azarhoosh, James Marchant, *Filterwatch*, 05/09/2018, "#nofilter? // How Iran Deals With Its Instagram 'Influencers'", available at: **http://bit.ly/3qqxJ6o**

74 "#IranVotes2017: Analysing The 2017 Iranian Presidential Elections Through Telegram, Twitter and Instagram", *Small Media*, available at: **https://bit.ly/3tXRjJM**

The COVID-19 quarantine started shortly before the Persian New Year, in March 2020. The quarantine meant plenty of free time for many to pass and an abundance of smart phones equipped with Instagram and other social media to resort to. During this time, Instagram played a significant role in diversifying the information about the pandemic and other socio-political topics, although nonetheless mixed with misinformation and disinformation. In particular, Instagram Live offered an unparalleled medium to Iranians to effectively launch private television channels, free of censorship. Celebrities, influencers, activists, media analysts, journalists, and even religious figures came together to discuss topics that are not typically allowed in the state-sanctioned media. Some of these conversations attracted up to 600,000 viewers – an unprecedented figure that underscores a significant shift in the public's preferences, and priorities for the type of content they seek.

Free from state monitoring, the editorial considerations of the media (including the diaspora media), and meticulous content moderation by platforms, Iranians took to Instagram to exchange ideas, connect with their fan base, and exercise freedom of expression like they did never before. In addition to breaking social and political taboos and offering unfiltered news and analyses, many influencers took this opportunity to enhance their follower network, promote commercial products and services, and maximize economic gains.[75] However, as in other parts of the world, some of these influencers attracted controversy because of their content's promotion of violence against women, misogyny, and in some cases, the abuse of minors.[76] Nevertheless, the latest Instagram Live debates are a testament to Instagram's role in diversifying public discourse and media plurality in Iran.

Instagram's popularity has not come without a cost, however. Online activities on Instagram have prompted periodic arrests of Iran-based influencers, often charged with "moral" crimes, undermining the state, and inciting the public. As discussed earlier, in May 2019, Iran's Police announced that it is compulsory for Iranian women who wish to be active on Instagram to wear hijab. While the enforceability of this rule is up for debate, it indicates the extent to which Iran is concerned with Instagram's influence on the lifestyle of Iranians. Additionally, in a June 2020 announcement, the police threatened that they carefully monitor Instagram Live videos, and will take legal action against those who violate the law.[77]

75 *BBC Persian,* 13/04/2020, "Instagram Live in Quarantine: From Entertainment and Education to Lectures and Interviews" [Persian], available at: **http://bbc.in/2OFxkzs**

76 Aida Ghajar, *Iranwire*, 26/04/2020 "Instagram Shuts Down the Account of Popular Iranian Singer Accused of Child Grooming", available at: **https://bit.ly/3pmKf66**

77 *KhabarOnline,* 24/06/2020, "Controversial Instagram Posts Under Police Magnifying Glass" [Persian], available at: **https://bit.ly/3iqSEn1**

From the state's perspective, the US-based Instagram not only threatens the ideological foundation of the Islamic Republic, but it also poses an existential threat to the IRIB and its monopoly over public multimedia productions, as well as its reach, influence, and revenue. These concerns have led to recurring debates among Iranian officials to block Instagram. With the election of a predominantly conservative parliament in February 2020, debates over the potential blocking of Instagram received renewed attention.

A ban on Instagram would represent an attempt by Iranian authorities to try and squeeze years of accumulated social and cultural forces back into Pandora's Box. Although political dissidents have largely been the target of online censorship up until this point, a ban on Instagram will have a different set of targets in mind: Instagram's thousands of young influencers, from restaurant critics, to dancers, to wisecracking comics. A ban will also ensure that footage of social and political suppression, for example the November 2019 protests, has less chance of being broadcast to the world. Nevertheless, Iranians have historically been resilient to censorship and found creative ways to bypass technical and political impediments to access unfettered information. With new restrictions in place and the prospect of blocking of Instagram, tech savvy Iranians will likely find new ways to mitigate the unfavorable effects of censorship.

7.2
TV ON-DEMAND

The rise of private online video and media sharing in Iran has not been without its share of political friction and debate. During the contested 2009 presidential elections, the campaign of reformist frontrunner Mir Hossein Mousavi launched an online television channel. It was almost immediately blocked by the Commission to Determine Incidents of Criminal Content (CDICC), the Judiciary's bureau for Internet filtering matters. Following the contested victory of the conservative incumbent, Mahmoud Ahmadinejad, the other reformist candidate, Mehdi Karoubi, announced his plans to launch a private television run by Behrouz Afkhami, a movie director and former member of parliament in the 1990s and early 2000s.[78] Afkhami was arrested by intelligence services and Karoubi's ambitions did not actualize. Less than a year later, Karoubi, along with Mousavi and his wife Zahra Rahnavard, were put under house arrest, which continues to date.

In a separate incident, in 2012, then Minister of Culture and Islamic Guidance, Mohammad Hosseini, asserted that running private televisions were not allowed under the law. At the time, Hosseini was reacting to initiatives by conservative figures and fractions to

78 Nahid Siamdoust, *LA Times*, 09/01/2006, "Iran Cleric Struggles to Get Alternative Views to TV Screens", available at: **http://lat.ms/3dckwuB**

run private televisions, some of which were solely Internet-based.[79]

The recurring stand-off with the government underscored the significance of IRIB's monopoly to the Islamic Republic, which is the uncontested propaganda arm of the Islamic Republic. Today, the IRIB maintains one of the best funded entities, with a budget as large as some of the ministries. Previous parliamentary efforts to revise the oversight rules and regulations that govern the IRIB have repeatedly failed. [80]

The IRIB has been adamant that it should be the sole regulating body responsible for licensing and overseeing the broadcast of video and music online — a position that has been strongly contested by Rouhani's administration. In a September 2015 letter to President Rouhani (as the head of the Supreme Council on Cyberspace), the Supreme Leader asserted that the IRIB was in charge of all matters related to multimedia content in cyberspace. The order was a first step to grant a significant amount of power to the IRIB in regards to online media production and broadcasting. [81]

The IRIB swiftly moved to cement its authority. It issued licenses for five entities to launch their Internet Protocol Televisions (IPTVs) in January 2016.[82] That same year, the IRIB sued Aparat, the most successful domestic video sharing platform similar to Youtube. Aparat was accused of operating illegally and without a license issued by the IRIB, the sole authority on matters of digital media, according to the organization's Statute and the Supreme Leader's order. The IRIB also established the nascent Organisation for Regulating Online Audio and Video (SATRA).[83]

In May 2016, the Cultural Commission of Iran's parliament proposed a policy that granted the right to regulate online multimedia content to IRIB. The proposal remained dormant until April 2018, when the conservative members of the commission announced that they had voted in favor of the IRIB's oversight on online multimedia content. The announcement prompted a staunch backlash from the reformist members of the committee and the ICT minister, who contested the lack of clear definitions of the audio and video content to be regulated by the IRIB.[84] Iran's parliament never voted on the policy passed by the committee. But the

79 "Iran's Minister for Culture and Islamic Guidance: No Private TV Licenses Will Be Given to Anyone" [Persian], available at: **http://bit.ly/39HABVA**

80 *Vigiato*, 8/05/2020, "What is SATRA? IRIB, Cyberspace, VOD, Regulatory and Other Issues" [Persian] available at: **https://vigiato.net/p/91423**

81 *Ibid*

82 *Taadol Newspaper,* 19/02/2017, "Positive Steps for Interactive TV Privatisation" [Persian] available at: **http://bit.ly/2KlRvR3**

83 *SATRA*, About Us [Persian], available at: **https://bit.ly/3nTSp4W**

84 *Vigiato*, 8/05/2020, "What is SATRA? IRIB, Cyberspace, VOD, Regulatory and Other Issues" [Persian], available at: https://vigiato.net/p/91423

policy represented the persistent will of conservatives to consolidate the IRIB's oversight power over all multimedia content.

In the meanwhile, SATRA continued to seal its authority over any multimedia content, virtual or otherwise. In 2018, the organization issued licences to four interactive TV stations (IPTVs) and seven audio and video media institutes.[85] SATRA also sought to establish itself as the governing authority over domestic Video-on-Demand (VOD) services. Previously, these services received their license from the Ministry of Islamic Culture and Guidance. Under the new governance rules, however, VOD platforms were required to obtain a secondary license from this new regulatory arm of the IRIB. The change prompted confusion among license applicants and prompted pushback from the government.[86]

In January 2020, Iran's Judiciary sought to consolidate the IRIB's power to regulate all multimedia content. The Head of the Judiciary, who is an appointee of the Supreme Leader, issued a letter that deemed any activity without appropriate licensing from the IRIB as unauthorized.[87] The government sharply criticized the judiciary for ruling on a matter outside of its jurisdiction, arguing that the issue falls within the mandate of the SCC.[88]

Most recently, in June 2020, the SCC, the ultimate Internet policy making body that reports to the Supreme Leader, announced its plans to arbitrate on the matter. To avoid further confusion and secure the best interest of domestic platforms, the SCC will hear arguments of the main stakeholders (i.e. the government and the IRIB), and consolidate its policy. [89]

The controversy highlights the growing political and financial importance of online broadcasting in Iran, which has been fuelling this ongoing power struggle between IRIB and the ICT Ministry. The IRIB is a key pillar of the Islamic Republic, which helps the regimes to maintain a monopoly over the flow of state-sanctioned information in multimedia format. Over the past decades, the Internet and foreign-based satellite televisions have undermined this monopoly. Iran's response to these external existential threats has been filtering the Internet, jamming of

85 *ISNA*, 03/05/2018, "Licenses for 4 Interactive TVs and 7 Audio Visual Media Institutions" [Persian], available at: **http://bit.ly/35ONegm**

86 *Vigiato*, 8/05/2020, "What is SATRA? IRIB, Cyberspace, VOD, Regulatory and Other Issues" [Persian], available at: **https://vigiato.net/p/91423**

87 Saeed Ebrahim Raisi, 18/01/2020,"Judiciary Directive" [Persian], available at: **https://bit.ly/3anTUoy**

88 *BBC Persian*, 26/01/2020, "Government criticises issuing of exclusive digital video and audio to IRIB" [Persian], available at: **http://bbc.in/3qjRGfs**

89 *Mehr News*, 12/06/2020, "The entrance of the SCC into the field of VOD" [Persian], available at: **http://bit.ly/2LHW3Sn**

satellite signals, and nationalization of cyberspace. The National Information Network (NIN) is the longest standing and most expensive project that seeks to centralize Iranians' access to state-sanctioned information by offering domestic content, platforms, services, and infrastructure.

Because the government has been historically in charge of the NIN's development, it has assumed control over the production and circulation of domestic multimedia content on this network. ICT Minister Azari Jahromi has particularly advocated for high quality productions to attract Internet users to domestic platforms via the NIN. According to the SCC spokesperson, domestic VOD platforms are required to dedicate at least 40% of their bandwidth to domestic content.[90] However, the IRIB considers Internet-based televisions in competition with its productions, affecting its viewership and monopoly over what type of content is permitted for broadcast. For online television networks, the unpopular IRIB's oversight means policing of content, lower quality of final productions, and, ultimately, reduced subscriptions and popularity.

In addition, these private online televisions are viewed as sources of generating additional revenue for any organization that oversees them. It is therefore no surprise that both the government and IRIB have been adamant about maintaining their grip over these platforms. In exchange for a license, the IRIB currently takes 50% of total revenue of online television networks and sues those who operate without a license.[91] And they seem to have the Judiciary on their side, too. The government, on the other hand, considers these platforms as attractive tools to lure Internet users to using the NIN infrastructure and services; a small concession of state control over content production, in return for the long term payoff gained by changing users' behavior and, effectively nationalizing the Internet.

Online television can play a significant role in breaking the IRIB's monopoly over multimedia content and a major leap toward media plurality in Iran. But the current governance of these platforms assumes a central role for IRIB to execute the state's policies and priorities. This stands against the principles of media plurality and democratic governance of the media. It remains to be seen which entity triumphs in the power struggle to secure oversight over these platforms.

90 *Peivast*, 22/02/2020, "Production of domestic content for VOD should reach 40%" [Persian], available at: **https://peivast.com/p/70466**

91 *Digiato*, 23/04/2018, "IRIB wants 50% of the revenue from audio and video activities" [Persian], available at: **https://bit.ly/3dlHZJT**

8 / ICT MARKET & THE DIGITAL ECONOMY

IN RECENT years, several state policies have been introduced, impacting Iran's ICT market as well as its growing start-up community. In particular, the government has sought to expand its oversight of the mobile market through a central database of all devices that enter the country. In addition, different measures are geared toward expanding public-private partnerships between the government and the startup community.

While these measures can help entrepreneurial projects thrive, they also pose unique challenges to users' right to privacy, in relation to product development and compliance with government requests for user data, among other issues. At the same time, after years of combatting circumvention tools, the Internet regulation body has passed new regulations that authorize the distribution of state-approved VPNs. Together, these policies show how far the state is willing to intervene in the digital market to secure its various objectives. This section takes a closer look at these interventions, and their implications for Iranian consumers.

8.1 MOBILE REGISTRY

In September 2017, the Rouhani administration formalized a new policy to combat the issue of smuggling electronic devices into Iran. Under this policy, the ICT Ministry established a central registry of mobile phone devices (HAMTA[92]) which requires information about all incoming mobile devices in the country to be submitted to the government. Failure to comply with this requirement within 31 days of purchasing a device, or bringing it to Iran (in the case of travelers), will lead to disconnection from Iran's phone service operators. The policy also affects travelers who wish to stay in Iran for longer than a month. If they wish to continue to use their personal device in Iran, travelers, including members of diaspora visiting the homeland, would need to register their phone data with the Iranian government.

The database asks for the International Mobile Equipment Identity (IMEI) number, make, and model of the device, and the SIM card number that will be associated with it. An IMEI is a phone's fingerprint — a 15-digit number unique to each device. Phone carriers and manufacturers share IMEI numbers to enable tracking of smartphones that may be stolen or compromised. The cost of registration varies according to the make and model of phone devices, ranging from $210 for iPhone 11 Pro Max 512 GB to $1 for NOKIA 105 (TA-1034) DS.[93] In the last year, more than 15

92 *HAMTA*, Website [Persian], available at: **https://hamtainfo.ntsw.ir/**

93 *Android Zoom*, 27/03/2020, "Price table of phone registration fees" [Persian], available at: **https://bit.ly/3pj4bGZ**

million mobile devices were registered in HAMTA.[94]

The policy claims to regulate the sales of imported devices, facilitate the collection of dues and tariffs from the mobile market,[95] and protect consumers against fraudulent activities. In short, the policy is designed to help the government to control the market and generate revenue. In reality, however, the seemingly protective measure has introduced additional costs to the buyer and disrupted the mobile market. In addition to the increase in customs fees that mobile vendors include in the final price, buyers also need to pay an additional cost to register newly purchased devices. Between September and October 2019, frustration about contradictory and confusing practices of the mobile registry office incited mass strikes of mobile vendors across Iran.[96] In recent months, with drastic fluctuations in the value of Iranian rial, these extra costs have renewed criticisms from buyers about the ultimate purpose that the registry serves. Some accuse the government of imposing additional costs to mitigate its budget deficit without offering any real protection against theft and fraudulent activities.

Aside from the costs, the political implications of the mobile registry have made many users uneasy. Personal anecdotes suggest that mobile users perceive the registry as a threat to their individual safety and an attempt to bolster Iran's surveillance apparatus. The lack of trust in the state to protect personal data, on one hand, and the obligation to register personal device information, on the other, continue to reflect in consumer discussions about the legality and implications of this policy.

8.2 START-UPS IN THE DIGITAL ECONOMY

Over the past decade, online businesses have seen a boom and a larger share in the digital economy. The improvement in high-speed Internet infrastructure, owing in part to the Rouhani government's increased investment in the industry, and the ubiquity of mobile Internet, particularly in urban areas, have facilitated this unprecedented growth. Everything from the prevalence of ride-sharing apps to the emergence of apps offering home-cooked meal deliveries illustrate that Iranian entrepreneurs are ready to take on the challenge of meeting consumers' needs.

The Rouhani administration has offered sustained support to the sector in different forms, from financial subsidies and facilitating data sharing to the Startup Action Plan, which was ratified

94 Arash Karimbeigi, Twitter, 02/07/2020, available at: **https://bit.ly/3s29VGV**

95 Raavi Network, Twitter, 03/1/2019, available at: **https://bit.ly/3b5Qfeh**

96 Iran International, Twitter, 08/10/2019, available at: **https://bit.ly/3jPgtWi**

by the cabinet on 19 May 2019.[97] The plan aims to provide start-ups with financial incentives, including a three-year tax break and the provision of co-working spaces to young companies. As of April 2020, the government has pledged to provide access to national databases (via APIs) to 70 startups that offer online services to their customers.[98]

But for all the opportunities this growth affords, the state's entanglements with the sector frequently fall short in offering businesses and users the protections they need, while overreaching in other areas — in places seemingly co-opting technologists into the state's surveillance apparatus. As discussed earlier, multiple forked versions of Telegram were taken down from Google Play last year due to their presumed connection to Iran's surveillance apparatus[99] (See **Section 6.1**). This incident highlights Iran's strategy of outsourcing surveillance duties to small private enterprises — something that may expand further as a result of Iran's ambitious eGovernment plans.

Another vulnerability in Iran's digital businesses concerns the failure to safeguard consumer data. Since April 2019, multiple major leaks of data belonging to Iran-based individuals have raised significant questions about the lack of clear judicial procedure for investigating such an incident. In April 2019, a dataset containing the information of around 300,000 drivers of the ride-sharing company Tap30 was leaked online.[100] In March 2020, 42 million records of user data were exposed through a forked version of Telegram that reportedly stored data on the Shekar System, an allegedly unverified search engine used by forked versions of Telegram, with permission from Iran's intelligence authorities.[101] The same leaker of the Telegram data also exposed 5 million users of SibApp, a domestic alternative to the AppStore for iPhone users in Iran (similar to what Cafe Bazaar is for Android users).[102]

Although Iran's proposed Data Protection Bill proposes an Office of Data Protection, such an office will only restore trust in private companies' handling of data so long as it acts as an exercise of regulatory powers. However,

97 Amir Nazemi, *Financial Tribune,* 24/05/2019, "Institutionalization for Multinational Cooperation in Iran Startup Ecosystem", available at: **https://bit.ly/3nVU5er**

98 *ITMEN*, 28/04/2020, "70 Start-ups have access to government APIs", available at: **http://bit.ly/38YPW5j**

99 Kaveh Azarhoosh, *Filterwatch*, 14/06/2019, "Slow-Downs and Start-ups — Privacy and the Digital Economy in Iran", available at: **http://bit.ly/3pn4JLO**

100 Lindsey O'Donnell, *Threat Post,* 19/04/2019, "Insecure Ride App Database Leaks Data of 300K Iranian Drivers", available at: **http://bit.ly/2ZjL2Kw**

101 *Radio Farda,* 02/04/2020, "ICT Ministry confirms that millions of internet users' information has been leaked", available at: **http://bit.ly/2NuhPK9**

102 *Bazarefanavari*, 01/04/2020, "After the disclosure of Iranian Telegram users' data; this time, the leakage of user data in Sib App", available at: **https://bit.ly/33NIR5e**

the Bill does not address exemptions for privacy on the basis of national security, a predominant threat to privacy under Iran's legal system.[103] The public's lack of faith in domestic businesses to securely host their private information was evident during the initial push for the widespread adoption of domestic messaging apps (See **Case Study 1**. The Blocking of Telegram; Two Years on).

Nonetheless, the vast majority of Iranian tech startups are not implicated in Iran's surveillance structure, nor are they set up to benefit from highly restrictive filtering regimes. As a result, tech startups could play a leading role in defining and protecting digital rights in Iran. There are two main ways they can do this: firstly, by refusing to work with government projects linked to surveillance.[104] And secondly, by improving their own data protection beyond the requirements of the government's proposed bill.

With government plans to expand Iran's eGovernment services significantly in the coming years, there is a possibility that more private firms will be called upon to deliver services that could in turn become part of the country's surveillance infrastructure. However, the startup communities' willingness to stand up for digital rights at this early stage could have a dramatic impact on the realisation of citizens' right to privacy. If the tech community fails to demand the establishment of an effective regulatory body that is capable of developing public trust in the private sector, then it is likely that many Iranian users will continue to opt for international service providers wherever possible.

8.3 LEGALISATION OF CIRCUMVENTION TOOLS

In April 2020, the General Secretary of Iran's Supreme Council of Cyberspace (SCC), Abolhassan Firouzabadi, announced the latest developments of the legal VPN project.[105] According to Firouzabadi, the Commission to Determine Incidents of Criminal Content (CDICC) recently concluded the first phase of this project that dealt with the legal aspects. The CDICC has reportedly passed new regulation that authorizes distribution of state-approved VPNs. The Commission operates under the office of Attorney General. It includes members from the legislative, executive, and judicial powers, as well as law enforcement and other state entities.

Moving forward, the Ministry of ICT will be in charge of implementation of the

103 *Filterwatch*, "Bills, Bills, Bills: Upcoming Policy Challenges in Iran, and How We Can Resist Them", available at: **http://bit.ly/2vDloBk**

104 Some tech companies have already illustrated willingness on this front. Last April, the Tehran-based taxi company Maxim, denied Tehran City Council access to the company's raw user data, stating that the privacy of its users is a red line they are unwilling to cross.

105 *ITIran*, 13/04/2020, "ICT Ministry is responsible for granting VPN licenses to eligible individuals" [Persian], available at: **http://bit.ly/3sz1fsz**

project and overseeing the distribution of legal VPNs via authorized operators. The ICT Ministry will determine who qualifies for these VPNs. According to Firouzabadi, examples of qualified applicants include startups, academic institutions, medical professionals, journalists, law enforcement, intelligence services, all of whom need to demonstrate "reasonable needs", for their request.[106] Additional approval from the Ministry of Cultural Affairs may be required.

Qualified applicants will then be approved to purchase VPNs legally. Otherwise, sales of circumvention tools remain illegal. Firouzabadi insisted that once legal VPNs are released to the market, illegal VPNs will be targeted more severely. In November 2019, the SCCS argued that the VPN economy had become so profitable for black market vendors that the SCC needed to step in and regulate this market.[107] Legal VPN will be priced by Iran's Regulatory Agency (IRA). However, concerns over the safety and security of these state-approved VPNs remain unresolved.

wFor decades, Iran has spent extensive resources on its filtering and censorship apparatus, including a national information network. Now the same apparatus is seeking to generate revenue off of filtering. By legalizing state-approved VPNs, Iranians can have access to uncensored information on the global Internet as long as they are willing to pay the government for it.

This approach to legal VPNs is in keeping with the other policy interventions we have discussed above in relation to the digital economy and digital markets. Iran's overriding objective across mobile registration, start-up investment, and legal VPN management has been control; typically expanding capacities for surveillance and monitoring, while extending the state's influence over ostensibly private sector actors, and driving forward the government's objective of fragmenting and localising Iranians' experience of the Internet.

106 *ITIran*, 14/04/2020, "How is a legal VPN granted to individuals and institutions?" [Persian], available at: **http://bit.ly/3oWCMLB**

107 *Zeitoon*, 12/11/2019, "Legal VPN for accessing forbidden sites" [Persian], available at: **http://bit.ly/3dfvpM1**

CONCLUSION

The year 1398 will be remembered as a crucial year in the development of Iran's localised Internet. The internet shutdown of November 2019 demonstrated once and for all that Iran's National Information Network project is not simply aimed at bringing Iranians online, or developing Iran's ICT sector as an end in itself; it is a programme of radical internet localisation.

Indeed, it is a project designed to make it easier to keep Iranians offline; to wean Iran's internet users off of the global Internet, and onto a national network where government surveillance and information controls are baked in. It's also a network where – in the event of a crisis – the shutters can come down, and Iranians can be closed off from the global community, without bringing the national economy to its knees.

Although authorities' radical localisation of the Iranian internet poses an immense threat to Iranians' digital rights, the decisions taken by policy-makers this year signpost further dangers ahead. The SCC's resolutions against internet privacy, and authorities' serious attempts at bringing forward a framework for "legal VPNs" all hint at momentum towards a complex "layered filtering" system, in which different citizens are granted different levels of access to the Internet. Accompanied by proposals for astonishingly intrusive systems linking National IDs to online activities, these decisions suggest an incoming assault on Iranian internet users' online privacy.

The Internet in Iran was once talked about as a great liberator, and a serious challenge to Iranian authorities' authoritarian approach to the media and human rights. If the last decade can be characterised as a cat-and-mouse game between authorities implementing, and users circumventing information controls, then we fear that 1398 may mark a departure point, as the year when Iranian authorities finally demonstrated their ability to not only censor the internet, but to exert real control over its underlying infrastructure, and to wield it as an effective tool for enforcing its authoritarian governance of online and offline civic space.

A FILTERWATCH REPORT

RESEARCH:
Kaveh Azarhoosh
Simin Kargar
Melody Kazemi
James Marchant

DESIGN:
Surasti Puri

JUNE 2021

FILTER WATCH