

Specific Instance Complaint

OECD Guidelines for Multinational Enterprises

Against:

Italtel Group SpA

Via Reiss Romoli - loc. Castelletto
20019 Settimo Milanese (Milano) Italy
Tel: +39 02 43881
Website: <http://www.italtel.com/>
CEO: Mr. Stefano Pileri
Email: stefano.pileri@italtel.com

Subject:

Italtel's breaches of human rights provisions of the OECD Guidelines in relation to an agreement between Italtel and the Telecommunication Company of Iran for provision of telecom services and technologies in the Islamic Republic of Iran

Complainants:

International Federation of Human Rights (FIDH)

17 Passage de la Main d'Or
75011 Paris, France
Tel: +33 1 43 55 25 18
Website: www.fidh.org

REDRESS

87 Vauxhall Walk
London SE11 5HJ, United Kingdom
Tel: +44 (0)20 7793 1777
Website: www.redress.org

Justice for Iran

Suite 8, 1 Abbey Street,
Eynsham, OX29 4TB, United Kingdom
Tel: +44 1865 880000
Website: www.justiceforiran.org

Contact person for Complainants:

Ms. Shadi Sadr
Executive Director of Justice for Iran
Email: shadis@jfingo.org

Presented to:

Italy National Contact Point

for the *OECD Guidelines for Multinational Enterprises*

Ministry of Economic Development

Directorate General for Industrial Policy, Competitiveness and SMEs

Division VI - International policies, promotion of corporate social responsibility
and the cooperative movement

Via Molise, 2

00187 Rome, Italy

Tel: (+ 39-6) 4705 3052

Fax: (+ 39-6) 4705 2013

Email: pcn1@mise.gov.it

Table of Contents

I. SUMMARY.....	4
II. INTRODUCTION	6
III. PREVIOUS ENGAGEMENT BETWEEN THE PARTIES	8
IV. WHAT IS AT STAKE.....	8
V. KEY BACKGROUND INFORMATION.....	15
1. Freedom of Expression and Internet in Iran.....	15
2. Relevant Publicly Available Information and Reports	19
3. IRGC and Cyber Army	24
4. IRGC’s Takeover of the TCI	26
VI. BREACHES OF THE OECD GUIDELINES	28
1. Failure to Conduct Risk-Based Human Rights Due Diligence	29
2. Failure to Identify the Full Scope and Severity of Potential Adverse Human Rights Impacts.....	31
3. Failure to Disclose Information Including Social Reporting.....	32
4. Failure to Promote Internet Freedom through Respect of Freedom of Expression Online	33
5. Other Potential Breaches	34
VII. OTHER RELEVANT INTERNATIONAL STANDARDS.....	35
VIII. REQUESTS TO THE NCP	37
Annex 1: Italtels’s Press Release	39
Annex 2: TCI’s Press Release	40
Annex 3: Complainants’ letters to Italtel.....	42
Annex 4: Small Media Report: Filterwatch, March 2017	45

I. SUMMARY

The present Complaint is submitted to the Italian NCP by the International Federation for Human Rights (FIDH), REDRESS, and Justice for Iran (JFI) (collectively referred to as the “Complainants”).

The Complainants allege that Italtel Group SpA (“Italtel”) has breached the *OECD Guidelines for Multinational Enterprises* (“OECD Guidelines”) in relation to a Memorandum of Understanding (“MoU”) entered into by Italtel and the Telecommunications Company of Iran (“TCI”) on 13 April 2016, whereby the parties agreed to purportedly “cooperate on the development of the Iranian telecommunications sector.”¹ The services offered by Italtel to TCI include “IP-NOC, IP-BB projects as well as provision of equipment for the implementation of the Iranian telecom network ... on the basis of the plans designated by TCI within 18 months.”² However, it is unclear whether this agreement has been formally executed and implemented and whether any services and/or equipment have so far been delivered to TCI.

As will be explained in section VI below, TCI is currently controlled by a consortium led by the Islamic Revolutionary Guard Corps (“IRGC”), which took over the company in 2009. Commanded by Iran’s Supreme Leader, the IRGC has been Iran’s most powerful military and security entity since its inception in 1979 in the aftermath of the Islamic Revolution. IRGC has played a crucial role in crushing political dissent and civil liberties throughout the country and more recently in cyberspace.

As such, the Italtel-TCI agreement, which aims to advance the infrastructure for TCI’s telecommunications and Internet services, risks to contribute to Internet censorship and suppression of a wide range of fundamental freedoms and human rights in Iran. The agreement would also empower and equip the IRGC with the tools to suppress opposition voices and commit serious human rights violations online and offline as detailed further in this complaint. By entering into the agreement with TCI, Italtel has partnered with one of the main violators of Internet freedom and freedom of expression in Iran, namely the IRGC, an entity which has been sanctioned by the US and the EU including for its record of human rights violations in Iran.

Therefore, it is respectfully submitted that, by entering into the MoU, Italtel has breached multiple principles of the OECD Guidelines by:

- i. failing to comply with its duty of due diligence as contemplated under the OECD Guidelines; it also failed to take reasonable steps and make good faith efforts to conduct human rights due diligence, including identifying the relevant factual circumstances and consulting with and preventing harm to affected communities, as part of its business decision-making and risk management systems;

¹ Press Release by Italtel entitled “Italtel and TCI Agree to Cooperate on Telecommunication Development Projects in Iran”, Tehran, 13 April 2016, available at: <http://www.italtel.com/content/uploads/2016/04/PR-Italtel-Iran.pdf>, accessed 5 September 2017. For a copy of the Press Release by Italtel please see Annex 1.

² Press Release by TCI entitled “TCI and Italtel Signed an MoU to Cooperate on Telecommunication Development Projects in Iran”, 17 April 2016, at: <https://www.tci.ir/en/News/ctl/ArticleView/mid/1669/articleId/2511/TCI-and-ItalTel-signed-an-MoU-to-cooperate-on-telecommunication-development-projects-in-Iran>, (no longer available) last accessed 2 February 2017. For a saved copy of the Press Release by TCI please see Annex 2.

- ii. failing to identify and conduct any *ex ante* assessment of potential, and in the circumstances foreseeable and arguably inevitable, adverse social and human rights-related impacts and risks associated with its planned business activities with TCI. Alternatively, it was willfully blind to frequent and well-documented occurrences of serious human rights violations committed by IRGC in cyberspace and within the telecommunications system. Italtel knew or should have known about the violations of the rights of the Iranian people to freedom of expression and information, as well as long-lasting and extensive violations of human rights, including the right to privacy, in which the IRGC, as the main shareholder of TCI, has been involved;
- iii. failing to disclose information about whether and which steps it is taking to identify and mitigate risks and potential adverse impacts in designing the services, technologies and potentially products it intends to provide to the TCI as per the MoU; and,
- iv. failing to promote internet freedom through respect of the rights to freedom of expression, assembly and association online.

Moreover, in the event and to the extent that the MoU shall be operable and enforceable and/or shall materialize into a definitive agreement between Italtel and TCI and/or shall be otherwise implemented, without Italtel having adequately met the above obligations, Italtel will have:

- i. engaged in close business cooperation with major violators of human rights in Iran relating to telecommunications and cyberspace, equipping them with more sophisticated and efficient means for perpetrating serious violations of the human rights against Iranian citizens and others subject to Iran's jurisdiction;
- ii. placed itself in a situation that would risk to cause Italtel to contribute or otherwise become complicit in the commission of serious violations of human rights committed or sanctioned by the Government of Iran through the IRGC, such as mass interception and surveillance of private communications, identification and persecution of human rights activists and citizens, systematic restriction of access to the Internet through extensive monitoring, filtering and blocking of internet content, etc.;
- iii. failed to exert leverage over its Iranian co-contractor, TCI, and indirectly over the IRGC, to address these issues as part of their modernization plan involving telecom and internet networks.

The Complainants submit that Italtel's abovementioned alleged conduct, which is further detailed and substantiated below, represents breaches to Chapters II (General Policies), III (Disclosure) and IV (Human Rights) of the OECD Guidelines. The specific provisions of the OECD Guidelines Italtel has breached are specified in section V below. The Complainants respectfully request that the Italian NCP offer its good offices to facilitate dialogue aimed at bringing Italtel's conduct in line with the OECD Guidelines. Should that dialogue fail to result in an agreement between the parties, the Complainants request that the Italian NCP investigate and make a determination as to whether Italtel has complied with the OECD Guidelines and to make appropriate recommendations to Italtel accordingly.

II. INTRODUCTION

The International Federation of Human Rights Leagues (FIDH), headquartered in Paris, is a non-partisan, non-sectarian, apolitical and not for profit organization. It federates 184 human rights organizations from 112 countries. Since 1922, FIDH has been defending all civil, political, economic, social and cultural rights as set out in the Universal Declaration of Human Rights. FIDH's work is directed at States as primary human rights guarantors. However, it also addresses non-State actors including multinational corporations.

REDRESS is an international human rights organization that seeks justice and reparation for torture survivors, headquartered in London and The Hague. REDRESS also aims to hold accountable the governments and individuals who perpetrate torture, and to develop the means of ensuring compliance with international standards and securing remedies for victims.

Justice for Iran (JFI) is a not-for-profit, non-governmental organization established in 2010 in London, UK. The mission of JFI is to address and eradicate the practice of impunity that empowers officials of the Islamic Republic of Iran to perpetrate widespread human right violations against their citizens, and to hold them accountable for their actions. JFI unravels the truth and seeks justice for ethnic and religious minorities, LGBTIs, women, and those who are persecuted because of their political beliefs. To achieve its mission, JFI researches, documents, validates, and litigates individual cases. It further raises public awareness and participates in human rights advocacy through the UN and the EU.

Italtel is a leading telecommunications company headquartered in Italy with operations across the world. It designs, develops, manufactures, and implements products and solutions for networks and next-generation communication services based on Internet Protocol (IP); Professional Services dedicated to the design and maintenance of networks; IT System Integration Services; Network Integration and migration activities. It offers proprietary products, engineering and network consultancy services, and managed services and solutions, such as Voice over IP (VoIP), unified communications and collaboration, HD video and interconnect solutions.

Italtel also provides Next Generation Data Centers and Mobile Broadband solutions as well as NetMatch-S, a cloud ready session border controller that offers functions to enable service providers to connect with VoIP networks. It is also specialized in building and transforming complex networks of a large number of international operators.

Italtel counts among its customers more than 40 of the world's top telecommunication operators and Service Providers (SP). Italtel currently operates in European, Middle Eastern, African and Latin American markets, providing digital transformation to large enterprises, public administrations and service providers in many countries including France, UK, Spain, Germany, Belgium, Poland, United Arab Emirates, Argentina and Brazil.

Telecommunications Company of Iran ("TCI") is Iran's main provider of Internet and mobile phone services, and the single fixed-line incumbent operator offering telecommunication and data services throughout the country. Established in 1971 as a public company, TCI was subject to the privatization scheme that took place in the 2000s. In 2009, subsequent to a highly contested bid, a consortium called *Tose'e Etemad Mobin*,

largely controlled by Iran's most powerful military and security entity the Islamic Revolutionary Guard Corps ("IRGC"), took over TCI by purchasing the majority share of the Company. As a result of this take over, as will be explained in more detail in section IV below, the IRGC now has full control over all telephone and Internet traffic in Iran.

According to an official Press Release published by Italtel, dated 13 April 2016 (see Annex 1), Italtel "has entered into a Memorandum of Understanding ("MoU" or "Italtel-TCI MoU") with Telecommunication Company of Iran ("TCI") to develop and modernize TCI's telecom network." It further states that "[u]nder the MoU, the parties have agreed to cooperate on the development of the Iranian telecommunications sector." Italtel CEO, Stefano Pileri, was quoted in the Press Release as stating that "[t]he MoU signed today represents a fundamental step forward in the cooperation between Italy and Iran and we are proud to be part of this important project."³

The MoU was signed during an official Italian Government mission to Iran led by the then Italian Prime Minister Matteo Renzi in April 2016. On the Iranian side, the MoU was signed by, and in the presence of, a number of TCI officials including Seyed Asadollah Dehnad, the Acting CEO; Ali Kargozar, CEO Deputy and Head of Technical and Commercial Operations Center; and Mostafa Seyed Hashemi, the Chairman of the Board of Directors.⁴ No further detail has been provided by the Italian party about this agreement since then.

In June 2016, Davood Zare'ian, the Spokesperson for TCI, announced that TCI had signed a EUR 1.0 billion finance agreement with an unnamed overseas vendor for the expansion and upgrade of its networks.⁵ He also confirmed that the MoU with Italtel has been successfully entered into and is now at the stage of "assessment by experts".⁶ The TCI has also announced that the telecom industry has been of particular interest for foreign investors, with rapid growth due to deregulation, licensing of new mobile virtual network operators (MVNOs), rollout of 3G and 4G services, and a start-up sector.⁷

It must be noted that these developments took place in the context of the recent lifting of a number of economic sanctions following the Nuclear Deal, also known as the Joint Comprehensive Plan of Action (JCPOA). In a recent report by Iran's Ministry of Foreign Affairs submitted to the National Security and Foreign Policies Commission of the Islamic

³ Press Release by Italtel entitled "Italtel and TCI agree to cooperate on Telecommunication development projects in Iran", Tehran, 13 April 2016, available at: <http://www.italtel.com/content/uploads/2016/04/PR-Italtel-Iran.pdf>, accessed 5 September 2017. See Annex 1.

⁴ Press Release by TCI entitled "TCI and Italtel Signed an MoU to Cooperate on Telecommunication Development Projects in Iran", 17 April 2016, at: <https://www.tci.ir/en/News/ctl/ArticleView/mid/1669/articleId/2511/TCI-and-ItalTel-signed-an-MoU-to-cooperate-on-telecommunication-development-projects-in-Iran>, (no longer available) last accessed 2 February 2017. For a saved copy of the Press Release by TCI please see Annex 2.

⁵ Iran-Italy Chamber of Commerce, 12 June 2016, available (in Farsi) at: <http://www.iiccim.ir/it/صورتجلسات/item/208-قرارداد-تل-ای-تال-با-ایران-مخابرات-208> accessed 5 September 2017.

⁶ Ibid.

⁷ Bloomberg, "Company Overview of Telecommunication Company of Iran", available at: <http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=115270>, accessed 5 September 2017.

Consultative Assembly (Iranian Parliament), the JCPOA was hailed for the following, which the complainants understand to be referring to the Italtel-TCI MoU:

1. "Signing MoUs and commercial agreements with leading telecommunications companies of the world in order to supply telecommunication equipment."
2. "Facilitating negotiations and making deals with advanced European countries in the area of telecommunication technologies."⁸

III. PREVIOUS ENGAGEMENT BETWEEN THE PARTIES

By letter dated 12 April 2017, a copy of which is annexed hereto (Annex 3), the Complainants communicated their concerns regarding the Italtel-TCI MoU to Italtel. The Complainants sought further information about the steps Italtel may have taken to ascertain the relevant human rights risks and to mitigate them. The Complainants also asked for a copy of the relevant provisions of the MoU describing the specific services and/or products to be supplied to TCI. The Complainants also requested information regarding any potential adverse impact assessment conducted by Italtel or any potential human rights due diligence plan put in place prior to engaging in further negotiations with TCI.

On May 23, 2017, having received no response to their correspondence, the Complainants wrote again to Italtel reiterating the request for information regarding the MoU. A copy of the letter is annexed hereto (Annex 3)

As of the date of this Complaint, no response has been provided by Italtel to these two correspondences.

IV. WHAT IS AT STAKE

While serious violations of human rights and state censorship in Iran did not start in 2009 with the take-over of TCI by the IRGC consortium, since the IRGC has increased its hold over the telecommunications sector, such human rights violations have become increasingly pervasive and alarming. Through the MoU, Italtel aims to equip TCI with more sophisticated means to monitor and control telecommunications and cyberspace. In particular, the infrastructure, services and technologies to be provided by TCI will allow the Islamic Republic's Ministry of Intelligence as well as the IRGC to more closely monitor, and, if deemed necessary, to shut down Internet traffic with increased efficiency. In other words, the MoU will further facilitate censorship, surveillance, and Internet shutdowns to quash dissenting voices in Iran.

⁸ Ministry of Foreign Affairs of the IRI, The Fourth Report Submitted to the National Security and Foreign Policies Commission of the IRI Parliament, 15 Jan 2017, p. 29, available at http://www.iribnews.ir/files/fa/news/1395/10/28/664017_177.pdf, accessed 5 September 2017.

Therefore, in entering into the MoU, Italtel provides more efficient means for the IRGC to continue perpetrating serious violations of the human rights of Iranian citizens. Indeed, the nature and subject of the MoU is such that in the context of Iran, a country with one of the worst records on Internet freedom in the world, it would inevitably contribute to more violations of human rights, particularly freedom of expression and privacy rights, through increased restrictions on telecommunication and Internet freedom.

Telecommunications is the largest non-oil sector in the Iranian economy. In Iran, the TCI has a monopoly over fixed-line infrastructure and is one of the largest Internet Service Providers (ISPs) in the country.

The Italtel-TCI MoU lays the ground for “cooperation on the development of the Iranian telecommunications sector” between “Italtel and TCI”.⁹ Although the specific services and/or products covered under the MoU have not been disclosed, Italtel’s 13 April 2016 Press Release specifically highlights the company’s credentials in the fields of “Network Functions Virtualization (NFV), managed services and all-IP communication solutions” and extensive experience in “building and transforming complex networks of a large number of international operators.”¹⁰

According to TCI, the MoU covers IP-NOC and IP-BB projects as well as the development and renovation of NGN (Next Generation Network) equipment and the new TCI value-added services with the world’s latest technology.¹¹ Under the MoU, Italtel is committed to providing the equipment and implementing the Iranian telecom network on the basis of the plans designated by TCI within an 18-month period.¹² Immediately below, we provide a brief description of some of the projects covered by the MoU, which may assist to provide a better understanding of what is at stake in this case.¹³

1. An **IP Network Operations Center (IP-NOC)** is a centralized location where administrators can directly supervise, monitor, and maintain a telecommunications network. It contains visualizations of the network that is being monitored, workstations at which the detailed status of the network can be seen, and the necessary software to manage the network.¹⁴ The main task of the IP-NOC is then to keep a watchful eye over

⁹ Press Release by Italtel entitled “Italtel and TCI agree to cooperate on Telecommunication development projects in Iran”, Tehran, 13 April 2016, available at: <<http://www.italtel.com/content/uploads/2016/04/PR-Italtel-Iran.pdf>>, accessed 5 September 2017 (See Annex 1); See also “Tehran, Rome Sign Telecoms Deal”, Financial Report, 16 April 2016, available at: <<https://financialtribune.com/articles/economy-sci-tech/39530/tehran-rome-sign-telecoms-deal>>, accessed 5 September 2017.

¹⁰ Ibid.

¹¹ Press Release by TCI entitled “TCI and Italtel Signed an MoU to Cooperate on Telecommunication Development Projects in Iran”, 17 April 2016, at: <<https://www.tci.ir/en/News/ctl/ArticleView/mid/1669/articleId/2511/TCI-and-ItalTel-signed-an-MoU-to-cooperate-on-telecommunication-development-projects-in-Iran>>, (no longer available) last accessed 2 February 2017. For a saved copy of the Press Release by TCI please see Annex 2.

¹² Ibid.

¹³ Here we are only commenting on two projects covered by the MoU: IP-NOC and IP-BB. As mentioned above, the MoU also covers other services including the development and renovation of NGN equipment and the new TCI value-added services. In the absence of further public information about these services it is difficult to evaluate the risks they may cause.

¹⁴ Margaret Rouse, Network Operations Center (NOC), available at: <<http://searchnetworking.techtarget.com/definition/network-operations-center>>, accessed 5 September 2017.

all monitored endpoints.¹⁵ It will allow monitoring of net-flows, hops, servers and endpoints attached to the networks. Additional IP-NOC capabilities include:

- email management services;
- backup and storage management;
- network discovery and assessments;
- policy enforcement;
- firewall monitoring and management;
- voice and video traffic management; and,
- performance reporting.¹⁶

This raises concerns about the scope of monitoring facilitated through the IP-NOC, which is exacerbated by the fact that an end-user is not aware of the IP-NOC's presence. IP-NOC technicians coordinate only with the IT service providers they are supporting, and do not interact directly with an end client. This is described as "silent partnership".¹⁷ Italtel's "silent partnership" with the TCI, and in turn with the government of Iran and IRGC, is aimed at providing further capability and an extra level of sophistication to the monitoring and filtering of internet content, including emails, voice and video traffic in Iran. As will be explained in further detail below, such practices can also contribute to more frequent and effectively targeted violations of the human rights of Internet users in Iran, including extrajudicial arrests, torture and persecution.

2. The **IP-BB project**, also known as "Internet Backbone" or "International Gateway", refers to the infrastructure that provides connectivity between a country and the global Internet. What makes this project a matter of concern is that state-directed implementation of national content filtering schemes and blocking technologies may be carried out at the backbone level, affecting Internet access throughout an entire country.¹⁸ In other words, those in control of the backbone are able to impose restrictions or maintain control over the flow of information. When practiced along with the centralization of the Internet, as has been the case in countries such as Iran, Egypt and China, this enables states to shut down the Internet during times of popular protest and political unrest.¹⁹

Internet users access the Internet through any number of networks, usually provided by ISPs, universities, or businesses. However, in order to reach content and communicate with others on the Internet, users often send traffic outside of the network of their ISP. Because the Internet is a system of interconnected networks, the path taken in this exchange of traffic can travel across several networks located in different countries before it reaches its final destination. These networks are provided with opportunities to control, survey, or manipulate the traffic that they are responsible for routing. In some

¹⁵ Continuum, "What Is a Network Operations Center (NOC)?", available at: <<https://www.continuum.net/msp-resources/mspedia/what-is-a-network-operations-center-noc>>, accessed 5 September 2017.

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ Open Net Initiative, "About Filtering", available at: <<https://opennet.net/about-filtering>>, accessed 5 September 2017.

¹⁹ "Choke Points: How countries like China and Russia are able to control the internet?", available at: <<https://qz.com/780675/how-do-internet-censorship-and-surveillance-actually-work/>>, accessed 5 September 2017.

countries including Iran, governments have maintained centralized control over critical networks, such as the infrastructure responsible for connecting the country to the rest of the world, creating what are known as “chokepoints”. These *chokepoints* provide additional control over the network, facilitating censorship, surveillance and shutting down of the Internet.²⁰

In the Iranian context, the TCI is the national level *chokepoint* through which all Internet traffic in and out of Iran travels.²¹ It is therefore a point at which the Islamic Republic authorities can perform filtering and prevent information from entering or leaving the country. Indeed, as will be explained in further detail below, in addition to the ongoing monitoring and filtering of the Internet, the Iranian government has on several occasions shut down the Internet to block posting or access to news, photos and videos e.g. about street protests during sensitive times of political unrest. As such, by providing the services contemplated under the MoU, Italtel will be (or is already) providing the IRGC with a firmer grip of the flow of information within the Iranian cyberspace, which will silence freedom of expression and violate privacy rights within Iran.

It is worth noting that the 2009 take-over of TCI by an IRGC-controlled consortium allows the IRGC to appoint the managing directors of TCI and make crucial decisions about the financial activities of TCI, including large-scale transactions such as the MoU with Italtel. As a result of this, the IRGC currently has full control over the entire telecom and Internet traffic in Iran. Further, the IRGC’s control of the TCI and other major mobile phone services secures their authority and influence over some of the most critical infrastructure of the Iranian Information and Communications Technology (“ICT”) sector (see Annex 4). As a result, IRGC’s direct access to all ICT infrastructure places IRGC in a position to access the data of millions of Internet users in Iran without the need to seek court permission or cooperation from other private or public bodies.

The IRGC is Iran’s most powerful military and security entity, having increasingly gained control over large stakes in Iran’s economy and significant influence over its political system. Since its establishment in 1979, the IRGC has played a central role in crushing political dissent and civil liberties through the means of widespread and systemic arrests, harassment, torture, and attacks against political activists, human rights defenders, cyber activists and journalists. As a result of IRGC’s demonstrated involvement in the Islamic Republic’s politics of oppression and repression, a number of individuals and entities linked to the IRGC have been subject to United States, European Union and international sanctions²², including by UN Security Council Resolution 1747.²³

Over the past decade, IRGC forces have become increasingly organized and engaged in the control of the cyberspace in Iran, particularly since the popular uprising that followed the 2009 presidential elections. More specifically, a recently published report by

²⁰ Ibid.

²¹ Ian Black, “How Iran is filtering out dissent,” *The Guardian* (UK), June 30, 2009, available at: <<https://www.theguardian.com/technology/2009/jun/30/internet-censorship-iran>>, accessed 5 September 2017.

²² See section IV.2 below for further information on US, EU and international sanctions against IRGC.

²³ UN Security Council, Security Council resolution 1747 (2007), 24 March 2007, S/RES/1747, available at: <https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf>, accessed 5 September 2017.

Article 19, the international watchdog of the right to freedom of expression, has analyzed how the IRGC, along with the Ministry of Intelligence, are closely involved in the administration of the Iranian Cyber Army (ICA) whose unidentified members are trained in cyber attacks, hacking and surveillance of Internet users.²⁴

There have been numerous cases involving extrajudicial arrests and detention, torture, and cruel and disproportionate punishments such as imprisonment or death sentence, in which the IRGC have used telecommunication networks and the Internet to either invade individuals' privacy to uncover information about them, or to identify and arrest them. Below are only few case studies documented in a 2017 Report by Justice for Iran and Small Media. See Annex 4 for the full report.

Case Study 1

An ordinary citizen was contacted over her mobile phone by an unknown person on an unknown number, who later turned out to be an official of the IRGC and appeared in the interrogation session, and asked to present herself for a briefing in relation to her internet activity. The citizen initially tried to avoid an interrogation session regarding her Internet usage, telling the officer that she was not in Iran. She was told that they knew she was in the country at that moment, and she was ordered to stop accessing a specific website, failing which she risked to be arrested and charged with collaboration with terrorists.

ICT Role

As all SIM cards must be registered under the name of the owner, the Intelligence Services may have obtained this individual's name and personal details and then pinpoint her via telecommunication towers. This method has been used in numerous cases, including against the prominent journalist and political activist Issa Saharkhiz when he was arrested following the 2009 disputed presidential elections.

Risk

The intelligence services, including the IRGC, have the power to locate persons perceived to be dissidents from the moment they turn on their phones, even if their phones are not smartphones.²⁵ Considering the IRGC's full control over TCI, they can pinpoint the location of the target without any permission from the judiciary being required.²⁶

²⁴ Article 19, "Tightening the Net, Part 2: The Soft War and Cyber Tactics in Iran", available at: <https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf> , pp. 6-7, accessed 5 September 2017.

²⁵ Small Media, Filterwatch, March 2017, p. 7 (See Annex 4 for the full report).

²⁶ Ibid.

Case Study 2

IRGC agents arrested a political activist while his phone calls were being intercepted by the IRGC. Shortly before his arrest, this activist had experienced unusual delays and disconnections during his phone conversations. He mentions that he tried calling his mother just before being arrested and had noticed that her voice disrupted strangely.

ICT Role

It is not unusual for IRGC to wiretap activists' phones and listen to or record their conversations over the phone. Following the IRGC's takeover of the TCI, it has become easier for the IRGC to tap phones and mobile conversations without the prior permission of the court.

Risk

As the IRGC is the main shareholder in many ICT companies such as TCI, Mobile-Telecommunication Company of Iran ("MCI"), and Taliya, it has the power to intercept a large proportion of communications via landline and mobile phone calls or SMS.²⁷

Case Study 3

A political activist was arrested and questioned by the IRGC, where he was presented with print-outs of his emails. His email had been hacked months before despite the fact that he had activated two-step verification by text message or SMS on his account.

ICT Role

As the activist had enabled two-step verification on his email account and he had obtained the code via SMS, the IRGC could get his password via a phishing attack, which is common practice for the Cyber Army, or by consulting the mobile phone service providers, such as TCI or MCI, who, as has already been described, can easily intercept the communication and provide IRGC with the verification code.

Risk

As the IRGC is the main shareholder in many ICT companies such as TCI, MCI, and Taliya, it has the power to intercept a large proportion of communications via phone calls or SMS. This power allows the IRGC to bypass important security features such as two-step verification.²⁸

²⁷ Ibid, p. 8.

²⁸ Ibid, p. 9.

In light of the above, there are sufficient and reasonable and sustainable grounds to believe that Italtel's services as contemplated under the MoU have the potential to reinforce TCI's technological capacity and infrastructure, including a more strategically centralized network architecture, thereby equipping the IRGC with more sophisticated and efficient means for perpetrating serious violations of the human rights of Iranian citizens relating to telecommunications and cyberspace.

The type of services and technologies to be provided by Italtel may further empower IRGC forces and other official and non-official organizations involved in the control and management of Iranian cyberspace to engage in an intensified crackdown on online expression and presence. This equates to further restrictions on information circulation, communications and expression of dissent, creating further obstacles to the work of organizations of the civil society, and will ultimately have a highly prejudicial and chilling effect on free expression and the sharing of information and ideas, especially for political groups, activists, human rights defenders, students and journalists.

The services to be provided by Italtel may also provoke a more pro-active approach of the IRGC and security services to Internet censorship, monitoring and hacking with more sophisticated technology and equipment. By including managed services and training, the Italtel-TCI MoU also lays the ground for the development of advanced domestic infrastructure for technical filtering and monitoring of the Internet, which will ultimately facilitate further Internet and telecommunication control. In sum, the MoU provides for a level of cooperation and development that may amount to contribution to, and complicity²⁹ in, adverse human rights impacts through its supply of services and products.

Furthermore, in the course of such close collaboration, Italtel would necessarily have real or constructive knowledge of the censorship, monitoring, and surveillance operations taking place within TCI, which exposes Italtel to knowingly participating in serious violations of freedom of expression, privacy rights and other fundamental human rights by its Iranian co-contractor, under the aegis of the IRGC. As set out in further detail below, these include censorship, filtering, and systematic monitoring and surveillance for the purposes of systematic repression, arbitrary arrest and unlawful prosecution of a large number of Iranian citizens. In fact, the potentially affected community encompasses an extremely large population, including political dissidents, human rights activists, religious and ethnic minorities, student activists, journalists, bloggers, youth, typical or average Internet users, and the population at large.

²⁹ We are relying here on the concept of "Complicity" as defined by the International Commission of Jurists. According to the ICJ the elements of complicity include: (1) Causation/Contribution, (2) Knowledge & Foreseeability, and (3) Proximity. See: Report of the International Commission of Jurists Expert Legal Panel on Corporate Complicity in International Crimes: Corporate Complicity Legal Accountability, available at: <<https://www.icj.org/wp-content/uploads/2012/06/Vol.1-Corporate-legal-accountability-thematic-report-2008.pdf>>; See also the 2005 Report of the UNHCHR which explains that a company is complicit in human rights abuses if "it authorizes, tolerates or knowingly ignores human rights abuses committed by an entity associated with it, or if the company knowingly provides practical assistance or encouragement that has a substantial effect on the perpetration of human rights abuses." (Report of the United Nations High Commissioner on Human Rights on the Responsibilities of Transnational Corporations and Related Business Enterprises with Regard to Human Rights, UN Doc E/CN.4/2005/91 (2005), para. 33.)

V. KEY BACKGROUND INFORMATION

1. Freedom of Expression and Internet in Iran

Since the inception of the Internet in the early 1990s, Internet access and online expression in Iran has been subject to extensive state-led censorship, filtering, monitoring and interference with those who would speak or act against the interests of the ideological values and discourse of the Islamic Republic of Iran. In the regional landscape, Iran has been reported as one of the most notorious violators of international standards relating to the Internet, namely freedom of expression and information, and right to privacy and protection of personal data.³⁰ As will be discussed throughout this section, numerous reports by Human Rights non-governmental organizations (NGOs) and international authorities have determined that Iran routinely violates human rights exercised online, and uses various technologies, tools and tactics, ranging from content production and control to invasive hacking, to restrict rights exercised offline.

The Iranian domestic legal framework governing the use of Internet and information technologies falls drastically short of relevant international standards relating to freedom of expression and privacy. The ambiguity of acts constituting crimes, the unjustifiable severity of sentences and the total disregard for the importance of freedom of expression in enabling protection of other human rights renders the current legal regime flawed. The latest piece of legislation, the *Computer Crimes Law*, adopted in January 2010, builds on the existing provisions of the Constitution of the Islamic Republic of Iran, the *Press Law* of 1986 and the *Islamic Penal Code*, providing for content-based restrictions on freedom of expression through use of technology, effectively repressing electronic and Internet-based expression.³¹

Since the 2009 political uprising, the Islamic Republic of Iran has strengthened its efforts to gain total political and ideological control over cyberspace in the course of what has come to be known as the Soft War in the Islamic Republic's political discourse. In several speeches delivered in the months following the June 2009 elections, the Supreme Leader Ayatollah Khamenei spoke of the urgent need to fight an ideological Soft War in the cultural and communication sphere: "Today, the country's priority is to fight the enemy's Soft War."³²

This "fight" and ideological control of cyberspace has been an ongoing battle and peaked in periods of political significance. For example, in the general election periods of June 2009 and June 2013, Internet connections and mobile phone services were completely

³⁰ For example, Reporters without Borders described Iran as one of the enemies of the Internet <<https://12mars.rsf.org/2014-en/2014/03/11/iran-the-revolutionary-guards-the-supreme-council-for-cyberspace-and-the-working-group-for-identifying-criminal-content/>>; similarly the Committee to Protect Journalists has also labeled Iran's Supreme Leader as one of the worst enemies of the freedom of press: <<https://cpj.org/reports/2000/05/enemies-00.php>> accessed 5 September 2017.

³¹ For more information, see Article 19, "Islamic Republic of Iran: Computer Crimes Law" (2012), available at: <<https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf>>, accessed 5 September 2017.

³² Official website of the IRI Supreme Leader, "Supreme Leader Meeting with Basij Members", November 2009, available at: <<http://farsi.khamenei.ir/news-content?id=8429>> accessed 5 September 2017.

severed by the Islamic Republic authorities and security forces, preventing communication and any reporting of events.³³

In a 2013 report by Article 19, it was clearly shown that there was a correlation between significant political events, such as general elections, and the tampering with the flow of information by the Iranian authorities.³⁴ The Article 19 report also documented how information control and policing of the Internet adversely affected the human rights of Internet users at various levels.³⁵ “It must also be noted that the censorship and policing of the Internet has multiple aspects including political, legal and technical. There are state departments and legislative and judicial bodies within the IRI government that provide the political and legal platform for the violations of basic rights and freedoms.”³⁶

Freedom House reported that “Iran continues to be an extremely dangerous environment for internet users. Iranian laws heavily restrict what is acceptable speech online and specify harsh punishments for those who deliberately flout restrictions, as well as those who have inadvertently drawn the ire of authorities.”³⁷ There are also technological and physical tools that make the control possible in real terms. It is in this area of telecommunications that we are witnessing the unfortunate and purely opportunistic contribution and complicity of international enterprises.

A 2013 report by Small Media further indicates that “Iran’s censorship apparatus is a product of overlapping legal jurisdictions, physical control over the few pathways for traffic to take out of the country, and the pariah status of Iran’s telecommunications sector in the eyes of international equipment vendors.”³⁸

In this context, three overlapping areas of governmental interference with individuals’ online activity, which compromises their right to freedom of information and expression and their right to privacy, can be identified:

1. Systematic control and restriction of content perceived as a threat to the ideological and political values of the Islamic Republic of Iran. This is done through extensive filtering and blocking of an estimated 25% of all websites worldwide³⁹, as well as bandwidth throttling⁴⁰, especially during times of popular protest and political unrest.⁴¹ The Iranian authorities have cracked down on

³³ Article 19, ‘Information Controls: Iran’s Presidential Elections’, available at: <https://asi19.org/cctr/iran-2013election-report/> accessed 5 September 2017.

³⁴ Ibid.

³⁵ Ibid.

³⁶ Ibid.

³⁷ Freedom House, Freedom of the Net 2015, available at:

<https://freedomhouse.org/report/freedom-net/2015/iran> accessed 5 September 2017.

³⁸ Small Media, “Iranian Internet Infrastructure and Policy Report: July-August 2013”, available at: <https://smallmedia.org.uk/sites/default/files/u8/iiipjuly.pdf> >, accessed 5 September 2017.

³⁹ Seifi, Farnaz, Internet in Ahmadinejad Term, Deutsche Welle, Oct. 2013, available at: <http://dw.com/p/19NCH> accessed: 5 September 2017.

⁴⁰ Throttling is a method of reactive censorship deployed by authorities to restrict access in response to short-term political or social events.

⁴¹ During the protests that followed the 2009 presidential elections, connection speed was slowed down to prevent the circulation of photos and videos. Webmail services such as Gmail were also significantly hindered. For more information see: Small Media’s 2014 report by Kyle Bowen and James Marchant: Revolution Decoded, Chapter 2: Internet Censorship In Iran: Preventative, Interceptive and Reactive; available at:

online activity by blocking a large number of leading media, news and popular websites such as Twitter and Facebook and by banning the use of most social media tools and platforms. Many sensitive terms are also blocked from showing up in search engine results.⁴²

2. Intrusive targeted measures of censorship through cyber attacks, hacking, malware, monitoring and Disturbed Denial of Service (DDoS) attacks carried out on political opponents and other targeted individuals.⁴³
3. Identification, monitoring and targeting of individual users who express dissent, including political dissident groups, social and human rights activists, journalists, bloggers, and Internet users at large.⁴⁴ These practices are not only in clear contradiction to the right to privacy, but have also led to arbitrary and at times extrajudicial arrests and persecution of individuals, as well as several cases of torture and ill-treatment in subsequent interrogations, as a result of which the authorities have succeeded in obtaining key information or communication, account details and web histories enabling the prosecution of targets of interest.

As such, these activities, because of their correlation with, and contribution to, a range of human rights abuses, violate a wide panoply of rights, given the deleterious impact these activities have on those rights; thus, they also infringe the right to be free from torture, the right to fair trial, and even the right to life, liberty and security in certain cases, in addition to the broad and systematic violations of privacy rights and right to free expression and information.

Below are several examples of infringement of freedoms and human rights of bloggers and users of social media by the Iranian authorities, more specifically the IRGC, as documented and reported by numerous sources:

<https://smallmedia.org.uk/revolutiondecoded/a/RevolutionDecoded_Ch2_InternetCensorship.pdf> accessed 5 September 2017.

⁴² The list of prohibited keywords originally only contained terms frequently used to access adult content, but this list has been expanded in the wake of the unrest that accompanied the 2009 presidential elections. See: Ibid, 9.

⁴³ See: Article 19, Tightening the Net, Part 2: The Soft War and Cyber Tactics in Iran, 2017, pp 31-7; available at: <<https://www.article19.org/resources.php/resource/38619/en/tightening-the-net-part-2:-the-soft-war-and-cyber-tactics-in-iran>> accessed 5 September 2017.

⁴⁴ In 2010 alone, 50 bloggers were arrested and prosecuted as an indirect result of their online activities, placing Iran in the bottom ten countries in Freedom House's index for online freedom of expression. See: Ibid; Freedom House, Freedom of the Press: Iran, 2010, available at: <<https://freedomhouse.org/report/freedom-press/freedom-press-2010>> accessed 5 September 2017.

Case study 4

An IRGC cyberspace specialist officer, Mostafa Alizadeh, announced in a statement on Iranian state television on February 1, 2015 that 12 Iranian Facebook users had been arrested on charges of “spreading corruption, and [carrying out a] mission to change family lifestyles.” He added that 24 other citizens were summoned to answer questions about their Facebook activities. Similarly, on January 31, 2015 a press release by the Center for Investigation of Organized Cyber Crimes, a subsidiary of the IRGC Cyber Defense Command, stated that several Facebook users had been arrested in a surveillance project by the IRGC named “Operation Spider” that is aimed at identifying and rooting out Facebook pages and activities that spread “corruption” and western-inspired lifestyles.⁴⁵

Case study 5

Soheil Arabi, a Facebook user, was arrested in November 2013 by the IRGC officers for his posts on Facebook and sentenced to death for “insulting the Prophet” (*sabb-al-nabi*).⁴⁶ It was after tireless campaigns and international outrage that his death sentence was recently struck down and commuted to seven and a half years in prison.⁴⁷

Case study 6

Iranian blogger Hossein Ronaghi Maleki was sentenced to 15 years in prison after an unfair trial by the Revolutionary Court, in which he was convicted of “membership of the internet group ‘Iran Proxy’”, “insulting the Supreme Leader” and “spreading propaganda against the system” in connection with articles on his blog.¹ After his arrest in 2009, he was held for 13 months in solitary confinement in Section 2A of Evin Prison, which is under the exclusive control of the IRGC, where he has said he was tortured. This included severe beatings by his interrogators from the IRGC who pressured him to make a televised confession.¹

⁴⁵ See: BBC Persian, ‘IRGC Arrested 12 Facebook Users in Operation Spider’, 2 February 2015, available at: <http://www.bbc.com/persian/iran/2015/02/150202_157_sepah_facebook> and International Campaign for Human Rights in Iran, ‘Iran’s IRGC Intensifies Crackdown on Facebook Users with 12 Arrests and 24 Summonses’, 5 February 2015, available at <<https://www.iranhumanrights.org/2015/02/facebook-arrests/>> accessed 5 September 2017.

⁴⁶ Human Rights Watch, ‘Iran: Death Sentence for Facebook Posts: Imminent Risk of Execution for Insulting the Prophet’, 2 December 2014, available at: <<https://www.hrw.org/news/2014/12/02/iran-death-sentence-facebook-posts>>; and Independent, ‘Iranian blogger found guilty of insulting Prophet Mohammad on Facebook sentenced to death’, 18 September 2014, available at: <<https://www.independent.co.uk/news/world/middle-east/iranian-blogger-found-guilty-of-insulting-prophet-mohammad-on-facebook-sentenced-to-death-9741572.html>> accessed 5 September 2017.

⁴⁷ See: Reporters Without Borders, ‘New arbitrary sentence for Facebook user who escaped death penalty’, as updated on 20 January 2016, available at: <<https://rsf.org/en/news/new-arbitrary-sentence-facebook-user-who-escaped-death-penalty>> accessed 5 September 2017.

2. Relevant Publicly Available Information and Reports

As described in further detail below, there is ample international recognition of the fact that the tools and tactics deployed by the Iranian authorities to implement and maintain control over telecommunications and cyberspace constitute unjustifiable limitations on the right to freedom of expression and the free flow of information. They also violate the right to be free from torture, the right to life, liberty and security, the right to privacy, having facilitated in many cases the persecution and oppression of political dissidents, minorities, human rights defenders and activists.

The situation of human rights in Iran in general and the freedom of expression and right to privacy in particular have been subjects of international concern for decades. The UN General Assembly has issued numerous resolutions raising deep concerns about, and condemning, human rights violations in Iran. Due to the gravity of the human rights violations in Iran, the UN Human Rights Council has recreated a country mandate.⁴⁸ The UN Special Rapporteur on the Situation of Human Rights in Iran (“UNSR on Iran”) has been constantly reporting to all UN member states on the human rights record of Iran over the past 7 years.⁴⁹ In her recent report, the UNSR on Iran indicated that:

“... at least 24 journalists, bloggers and social media activists were reportedly either in detention or sentenced for their peaceful activities as of 13 December 2016 and reports suggest that many others are regularly subjected to interrogations, surveillance and other forms of harassment and intimidation. The Special Rapporteur has also received reports indicating that the Government continues to place restrictions on access to information by filtering websites, intimidating and prosecuting Internet users, bloggers and social media activists, and throttling Internet speeds. According to these reports, some 5 million websites remain blocked in the country, with the top 500 blocked websites dedicated to the arts, social issues, news and other popular culture issues.”⁵⁰

Since 2011, the Council of the European Union, of which Italy is a member, has unambiguously adopted the Regulations imposing restrictive measures in view of the situation of human rights in Iran, including:

- **Asset freeze and visa bans** for individuals and entities responsible for grave human rights violations.

⁴⁸ Resolution 16/9 adopted by the Human Rights Council on the Situation of human rights in the Islamic Republic of Iran, 8 April 2011, A/HRC/RES/16/9, available at: <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Pages/ListReports.aspx> accessed 5 September 2017.

⁴⁹ See the webpage of the UN Special Rapporteur on the situation of human rights in the Islamic Republic of Iran, available at: <http://www.ohchr.org/EN/HRBodies/SP/CountriesMandates/IR/Pages/SRIran.aspx> accessed 5 September 2017.

⁵⁰ Report of the Special Rapporteur on the situation of human rights in the Islamic Republic of Iran, March 2017, A/HRC/34/65, para. 52, available at: <http://www.refworld.org/docid/58bd7e2b4.html> accessed 5 September 2017.

- **Ban on exports** to Iran of equipment which might be used for internal repression and of equipment for monitoring telecommunications.⁵¹

Among the 82 individuals currently subject to the EU sanctions, a dozen of them are commanders or other high-level authorities of the IRGC or officials who have played a part in violations of Internet freedom and the right to privacy. Of particular importance to this case:

- i. Reza Taghipour, “Member of the Supreme Cyberspace Council and Former Minister for Information and Telecommunications. He was one of the top officials in charge of censorship and control of Internet activities and also all types of communications (in particular mobile phones). During interrogations of political detainees, the interrogators make use of the detainees' personal data, mail and communications. On several occasions following the 2009 presidential election and during street demonstrations, mobile lines and text messaging were blocked, satellite TV channels were jammed and the Internet was locally suspended or at least slowed down.”⁵²
- ii. Mehrdad Omid, “Former Head of the Computer Crimes Unit of the Iranian Police. He is responsible for thousands of investigations and indictments of reformists and political opponents using the Internet. He is thus responsible for grave human rights violations in the repression of persons who speak out in defense of their legitimate rights, including freedom of expression.”⁵³
- iii. Abdolsamad Khoramabadi, “Head of the “Commission to Determine the Instances of Criminal Content”, a governmental organization in charge of online censorship and cyber crime. Under his leadership the Commission defined “cybercrime” by a number of vague categories that criminalize creation and publication of content deemed inappropriate by the regime. He is responsible for repression and the blocking of numerous opposition sites, electronic newspapers, blogs, sites of human rights NGOs and of Google and Gmail since September 2012. He and the Commission actively contributed to the death in detention of the blogger Sattar Beheshti in November 2012. Thus the Commission he is heading is directly responsible for systemic violations of human rights, in particular by banning and filtering websites to the general public, and occasionally disabling Internet access altogether.”⁵⁴

⁵¹ The last update, from 11 April 2017, extended the restrictive measures until 13 April 2018; see: Implementing Regulation 2017/685 of 11 April 2017 implementing Regulation (EU) No 359/2011 and Council Decision (CFSP) 2017/689 of 11 April 2017 amending Decision 2011/235/CFSP. Also see: Council of the EU, Press Release 199/17, 11 April 2017, available at <www.consilium.europa.eu/press-releases-pdf/2017/4/47244657655_en.pdf> accessed 5 September 2017.

⁵² Council of the EU, Council Implementing Regulation (EU) 2016/556 of 11 April 2016, Official Journal of the European Union, L 96/3, available at: <<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0556&qid=1460465337598&from=EN>> accessed 5 September 2017.

⁵³ Ibid.

⁵⁴ Council of EU, Council Implementing Regulation (EU) No 206/2013 of 11 March 2013 implementing Article 12(1) of Regulation (EU) No 359/2011, Official Journal of the European Union, L 68/9, available at: <<http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013R0206&qid=1483494900885>> , accessed 5 September 2017.

The one Iranian entity that is currently subject to EU sanctions is also the Cyber Police (aka: FATA)⁵⁵, which was established in 2011 to monitor and prosecute potential cyber criminals. The Iranian Cyber Police is a unit of the Islamic Republic of Iran Police, previously headed by Esmail Ahmadi-Moqaddam. According to press reports, police chief Ahmadi-Moqaddam underlined that the Cyber Police would take on anti-revolutionary and dissident groups who used Internet-based social networks in 2009 to trigger protests against the re-election of President Mahmoud Ahmadinejad.⁵⁶

These measures are regularly updated and the complainants expect them to remain in place for the foreseeable future. The last update, from 11 April 2017, extended them until 13 April 2018.⁵⁷ While some nuclear-related sanctions against Iran were lifted in January 2016, human rights related sanctions remained in place.⁵⁸ In addition to the extension of the asset freeze and visa bans for human rights violators, the Council of the EU has kept in place the prohibitions to sell, supply, transfer or export equipment or to provide technical assistance, whether directly or indirectly, to entities in Iran in relation to goods and technology which might be used for internal repression or for monitoring telecommunications.⁵⁹

Freedom of expression in Iran remains a concern for many governments. During the first and second cycles of Universal Periodic Review (UPR) of the UN Human Rights Council in 2009 and 2014, Italy, alongside some other member states, made a number of recommendations to the Islamic Republic regarding freedom of expression and the rights of the detainees (e.g. public protesters and journalists):

- “Fully guarantee the right to freedom of expression, press and political activity”⁶⁰
- “With regard to those arrested after the presidential elections, fully respect the right to a fair trial of all persons under arrest and detainees...”⁶¹

⁵⁵ In Farsi, *Polis-e fazaye toleed va tabadol-e etela'at* (FATA). See website at: <<http://www.cyberpolice.ir/>> accessed 5 September 2017.

⁵⁶ Council of EU, Council Implementing Regulation (EU) No 206/2013 of 11 March 2013 implementing Article 12(1) of Regulation (EU) No 359/2011, Official Journal of the European Union, L 68/9, available at: <<http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013R0206&qid=1483494900885>>, accessed 5 September 2017.

⁵⁷ Council of the EU, Council Implementing Regulation (EU) 2017/685 of 11 April 2017 implementing Regulation (EU) No 359/2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran, Official Journal of the European Union, L 99/60, available at: <<http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32013R0206&qid=1483494900885>>, accessed 5 September 2017.

⁵⁸ Ibid.

⁵⁹ See: Council of the EU, Press Release 199/17, 11 April 2017, available at <www.consilium.europa.eu/press-releases-pdf/2017/4/47244657655_en.pdf> accessed 5 September 2017.

⁶⁰ UPR Info, Database of Recommendations, search for Iran as the State Under Review, available at: <<https://www.upr-info.org/database>> accessed 5 September 2017.

⁶¹ Ibid.

Similar concerns were shared by other states including Sweden, France, Germany and The Netherlands who made recommendations about the Internet censorship and crackdowns on civil society in Iran.⁶²

Moreover, in a report by the Home Office of the United Kingdom it was stated that the Iranian authorities “(...) harass, detain, abuse, torture, and use vaguely worded criminal provisions to prosecute, flog and otherwise severely punish publishers, editors and journalists. This also includes those involved in internet-based media, such as bloggers and users of social media, where their reporting is, or is perceived to be, critical of the government or offensive to public morality. Perceived government critics including journalists and bloggers are at risk of torture and are likely to be held in poor detention conditions, some of which are capable of breaching the Article 3 ECHR threshold.”⁶³

These concerns, however, are not limited to European states. In addition to restrictive measures against certain persons with respect to grave human rights abuses by the government of Iran⁶⁴, the US State Department (“USSD”) has been publishing annual human rights reports covering the situation of human rights in the world. The USSD Country report on Human Rights Practices in Iran for 2015 noted that “[t]he most significant human rights problems were severe restrictions on civil liberties, including the freedoms of assembly, association, speech (including via the internet), religion, and press. (...) Other reported human rights problems included disregard for the physical integrity of persons, whom authorities arbitrarily and unlawfully detained, tortured, or killed; disappearances; cruel, inhuman, or degrading treatment or punishment, including judicially sanctioned amputation and flogging; (...) arbitrary arrest and lengthy pretrial detention, sometimes incommunicado; continued impunity of the security forces; denial of fair public trial, sometimes resulting in executions without due process; the lack of an independent judiciary; political prisoners and detainees; (...) arbitrary interference with privacy, family, home, and correspondence; harassment and arrest of journalists; censorship and media content restrictions.”⁶⁵

The report further notes that “[t]he government ... requires all owners of websites and blogs in the country to register with the ministry, which, along with the Ministry of Information and Communications Technology, the Ministry of Intelligence and Security, and the Tehran Public Prosecutor’s Office, compose the Committee in Charge of Determining Unauthorized Websites, the governmental organization that determines censor-

⁶² Ibid.

⁶³ Home Office, “Country Policy and Information Note on Iran: Journalists and Internet-based Media”, October 2016, available at:

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/565823/CPIN-Iran-Journalists-and-internet-based-media-v2-October-2016.pdf> accessed 5 September 2017.

⁶⁴ Executive Order 13606 Blocking The Property And Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria Via Information Technology, 22 April 2012, available at: <<https://www.treasury.gov/press-center/press-releases/Pages/tg1547.aspx>>, accessed 5 September 2017.

⁶⁵ US State Department, Country report on Human Rights Practices for 2015- Iran, 13 April 2016, available at: <<http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm?year=2015&dliid=252923>>, accessed 5 September 2017.

ing criteria. ... the Press Supervisory Board and judiciary invoked the law to close websites during the year.”⁶⁶

International NGOs have also been monitoring and raising alarms about the deficit of fundamental rights and basic freedoms in Iran. For example, Internet freedom in Iran has been categorized as “Not Free” and among the worst performers worldwide in every single annual report by Freedom House.⁶⁷ Freedom House’s report “Freedom on the Net 2015” found that social media and ICT Apps in Iran, as well as political and social content, were blocked, and bloggers and ICT Users were arrested. The report also noted that “[t]he Iranian authorities continued to restrict access to tens of thousands of websites in 2014-2015, particularly those of international news sources, the opposition, ethnic and religious minorities, and human rights groups. Websites are also filtered if they differ from the official doctrine of the state’s Islam (...) The online sphere is heavily monitored by the state in Iran. Both Iranian Cyber Police (FATA) and the Information and Communications Technology Ministry have announced that they are capable of monitoring all messages sent on messaging apps Viber, Tango, and WhatsApp.”⁶⁸

Freedom House’s “Freedom on the Net 2016” similarly noted that “[t]ens of thousands of websites remain filtered, including news sites and social media, which have otherwise become a relatively free platform of expression for many Iranians”⁶⁹ and that “the wholesale blocking of social media websites including YouTube, Twitter, and Facebook, and surveillance of the activities of Iranians who manage to reach such platforms, remained in effect in 2015. In January, the IRGC’s cybercrime unit confirmed the existence of an extensive Internet surveillance program believed to have been initiated the previous year. The unit said that more than 130 Facebook pages had been taken down as part of the operation, and that more than 30 individuals had been arrested or detained.”⁷⁰

Amnesty International’s annual report for 2015/2016 also noted that “in August, the Ministry of Communications and Information Technology announced the second phase of “intelligent filtering” of websites deemed to have socially harmful consequences, with the support of a foreign company. The authorities continued efforts to create a “national internet” that could be used to further impede access to information via the internet, and arrested and prosecuted those who used social media to express dissent. In June, a spokesperson for the judiciary said that the authorities had arrested five people for “anti-revolutionary” activities using social media, and five others for “acts against decency in cyber-space”.”⁷¹

⁶⁶ Ibid.

⁶⁷ Freedom House, “Freedom of the Net 2015”, available at: <https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf> ; and “Freedom of the Net 2016”, available at: <<https://freedomhouse.org/report/freedom-press/2016/iran>> accessed 5 September 2017.

⁶⁸ Ibid.

⁶⁹ Freedom House, “Freedom of the Net 2016”, available at: <<https://freedomhouse.org/report/freedom-press/2016/iran>> accessed 5 September 2017.

⁷⁰ Ibid.

⁷¹ Amnesty International, “Annual Report on Iran 2015/2016”, 24 February 2016, available at: <<https://www.amnesty.org/en/countries/middle-east-and-north-africa/iran/report-iran/>>, accessed 5 September 2017.

The above sources as well as further reports from other governmental and non-governmental sources have been publicly available and easily accessible, including from the UK FCO and NGOs such as JFI, FIDH and HRW.⁷²

3. IRGC and Cyber Army

The IRGC was established in 1979 as a militia. Over the following decades it transformed into a parallel national army and security force, which also branched out into the economy.⁷³ In addition to military and security projects, the IRGC is now involved in various areas of Iran's economy, such as construction, energy, and, more importantly for the purpose of the present Complaint, telecommunications.⁷⁴

The IRGC has a long history of breaching the right to freedom of opinion and expression, the right to freedom of information, the right to privacy and protection of personal data, and the right to free access to the Internet.⁷⁵ Such violations have been carried out through various branches and departments of the IRGC, chief among them the Centre for the Investigation of Organized Crime (CIOC), also known as the Cyber Crime Office.⁷⁶

Established in 2007, the CIOC is a division of the Intelligence Office of the IRGC operating under the Revolutionary Guard Cyber Defence Command (RGCDC). Since its inception, the CIOC, officially operating under direct control of the IRGC, is in charge of ensuring the security of the Islamic Republic of Iran in cyberspace. More specifically, the CIOC is responsible for monitoring and investigating organized crime, terrorism, espionage, and economic and social crimes in cyberspace. In collaboration with other intelligence organizations and judicial bodies, it identifies threats posed by the Internet and other advanced technologies by making use of the intelligence and technical capabilities of the IRGC forces and experts, thus assisting the IRGC in its "role of protecting the Revolution and its achievements".⁷⁷

In the course of one of its earliest projects, the CIOC carried out the arrest, interrogation, and prosecution of individuals unfoundedly accused of having contributed to the development of websites with pornographic content. While these individuals were held in de-

⁷² See for example: Foreign & Commonwealth Office, Human Rights & Democracy :The 2016 Report, at 39, available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/630623/Human_Rights_and_Democracy_Report_2016_accessible.pdf accessed 5 September 2017.

⁷³ See for example: CNBC, Revolutionary Guard Has Tight Grip on Iran's Economy, 8 Dec 2010, available at: <https://www.cnbc.com/id/40570657> accessed 5 September 2017.

⁷⁴ For example see: *Digarban*, "The Revolutionary Guards is entering the IT market," [in Farsi only], December 12, 2011, available at: <http://www.digarban.com/node/3715> accessed 5 September 2017.

⁷⁵ For example see the case of Arash Sadeghi who was arrested and interrogated by IRGC members on charges such as "spreading propaganda against the system" and "insulting the founder of the Islamic Republic". The evidence presented by the interrogators from IRGC to support the charges against him consisted of printed copies of his Facebook messages and e-mails to journalists and human rights activists abroad (Source: Report of the Special Rapporteur on the situation of human rights in the Islamic Republic of Iran, 17 March 2017, A/HRC/34/65, available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_65_AEV.docx accessed 5 September 2017).

⁷⁶ In Farsi, *Markaz-e baresi-e jarayem-e sazman yâfteh*. More information available at:

<http://www.gerdab.ir/fa/about> , accessed 5 September 2017.

⁷⁷ Article 150 of the Constitution of the Islamic Republic of Iran.

tion, the Islamic Republic of Iran Broadcasting (IRIB) broadcasted forced confessions of a number of the accused. In the televised confessions, the accused admitted that they intended to attack the cultural basis of the Islamic Republic through corrupting the youth and advancing political agendas against the government or Islam. They further admitted that they received money from the government of the United States to develop websites with pornographic content. While none of these accusations were substantiated by evidence, different branches of the Revolutionary Court issued sentences against the accused, ranging from multiple years of imprisonment to the death sentence. It took several years for some of the accused or their relatives to break their silence about the severe physical and psychological torture and ill-treatment they endured prior to the confessions, details of which have been documented by Justice for Iran in a report published in June 2012.⁷⁸

Furthermore, the CIOC played an important role in the post-2009 Presidential election events in identifying, arresting and sentencing protestors, journalists and cyber activists caught up in the post-election unrest, particularly those active in cyberspace. Attacks on websites and email accounts of activists peaked following the disputed election. In its June 2012 report, Justice for Iran documented details of widespread and severe violations of human rights by the authorities and officials of the IRGC Intelligence Office, in particular the CIOC.⁷⁹

Since 2009, the CIOC has systematically identified and arrested individuals who have produced content on cyberspace deemed to be “criminal” by the CIOC. Such content includes insulting the religion of Islam or officials of the Islamic Republic, proselytizing the Baha’i faith, propagating Sufism, denouncing state-sanctioned discrimination against the ethnic and other minorities within Iran, using the Internet to establish anti-Islamic Republic political groups, publishing methods of circumventing the filtering imposed by the Islamic Republic in order to access censored websites, as well as re-posting of or linking to content from censored websites.⁸⁰

The CIOC closely collaborates with a unit of the Iranian Police established and controlled by the IRGC, namely the Iranian Cyber Police (also known as FATA or Police in charge of the Sphere of Production and Exchange of Information⁸¹), as part of what has become to be known as the Iranian Cyber Army (ICA).

As reported in a recent two-volume report published by Article 19⁸², the IRGC, alongside the Ministry of Intelligence, are closely involved in the administration of the Cyber Army. In an article published in May 2010 by Fars News, a news agency controlled by the IRGC, Brigadier Ebrahim Jabbari, the commander of the *Ali-ibne-Abitaleb* Brigade, stated that

⁷⁸ “*Gerdab: A Dictated Scenario*” (June 2012), at pp. 23-36, available at: <http://justice4iran.org/issues/torture-issues/gerdab-a-dictated-senario/>, accessed 5 September 2017.

⁷⁹ *Ibid.*, at pp. 26-30.

⁸⁰ *Ibid.*

⁸¹ In Farsi, *Polis-e faze toleed va tabadol-e etela’at*, see website at: <http://www.cyberpolice.ir/>, accessed 5 September 2017.

⁸² Article 19, ‘Tightening the Net: Internet Security and Censorship in Iran, Part 1: The National Internet Project’, available at: https://www.article19.org/data/files/The_National_Internet_AR_KA_final.pdf and ‘Tightening the Net, Part 2: The Soft War and Cyber Tactics in Iran’, available at: https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf accessed 5 September 2017.

“[t]oday we witness the successful creation of the ICA by the IRGC forces. Our Cyber Army ranks as second in all the world.”⁸³

In September 2011, Mashregh News, a website with close ties to the IRGC, reported that “IRGC is the authority responsible for policing Iranian cyberspace. In 2009, this powerful arm of the Iranian armed forces took responsibility for controlling the National Internet and has continued doing so ever since. [The] IRGC has established a Cyber Police that oversees the Internet and its users in the country.”⁸⁴

While attacks on websites and email accounts of activists peaked following the 2009 disputed Presidential elections in Iran, but nevertheless, the attacks have been part of a continuing and sustained campaign. In 2013, Justice for Iran's website was hacked several times by the Cyber Army. Ever since there have been further cyber attacks and attempted hackings against the directors of Justice for Iran.

4. IRGC's Takeover of the TCI

In 2009, two IRGC-owned companies together with Execution of Imam Khomeini's Order (EIKO, also known as Setad), a foundation owned and controlled by the Supreme Leader of Iran,⁸⁵ formed a consortium called *Tose'e Etemad Mobin*, itself dominantly owned and controlled by the IRGC.⁸⁶ The Consortium then took part in a bid to buy the majority shareholding of TCI and won the bid. This became an immediate cause of controversy as a number of other companies claimed the auction was rigged in favor of the Consortium.⁸⁷

A 2016 report published by an Iran-based specialist IT journal revealed the breakdown of the shareholders of the TCI following the 2009 purchase.⁸⁸ The report criticizes the so-called ‘privatization’ of the TCI and stresses that there is no doubt that the Consortium purchased the majority share of TCI is owned by IRGC and Setad. The report also gives a detailed account of the dominance of a complex network of companies over the ICT sector in Iran, the majority of which are controlled by the IRGC.⁸⁹

Having purchased 50% plus one of the shares, and therefore holding the majority share

⁸³ Fars News, 20 May 2010, available (in Farsi) at: <http://www.farsnews.com/newstext.php?nn=8902300353> accessed 5 September 2017.

⁸⁴ Mashregh News, What Does a 250,000 Member ICA Have in Mind, September 2011, available at: <http://www.mashreghnews.ir/fa/print/64789> accessed 5 September 2017.

⁸⁵ A 2013 Reuters investigative report has documented how Setad has built a multibillion dollar empire on the systematic seizure of thousands of properties belonging to members of religious minorities like Baha'i, as well as political dissidents and other Iranians living abroad. See: Reuters, Khamenei controls massive financial empire built on property seizures, Nov 11, 2013, available at: <http://www.reuters.com/investigates/iran/#article/part1> accessed 5 September 2017.

⁸⁶ ICTNA, “The Characteristic of Etemad Mobin Consortium as the Buyer of Communications Stocks Explained”, September 12, 2009, available (in Farsi) at: <http://www.ictna.ir/id/022937/> accessed 5 September 2017.

⁸⁷ ICTNA, “Behind the Curtain of Security-related Disqualification of Pishgamana-Kavir-Yazd in the TCI Auction: In Conversation with PKY's CEO” Oct 26, 2009, available (in Farsi) at: <http://www.ictna.ir/report/archives/023756.html> accessed 5 September 2017.

⁸⁸ Meysam Qasemi, “Humble Owners of ICT”, Peyvast Monthly, Sep 2016, available at: <http://peivast.com/month-report/مالکان-فروتن-ict/> accessed 5 September 2017.

⁸⁹ Ibid.

of TCI, it can be safely argued that the IRGC-controlled Consortium now controls TCI. This, in practice and under Iran's Commercial Code, means that the CEO as well as the Chairperson and majority of the members of the Board of Directors are now appointed by the IRGC-controlled Consortium. The same Consortium and its appointees then have authority to make crucial decisions about the transactions and financial activities of the TCI, including the MoU with Italtel.

The ever-increasing grip of the IRGC on the telecommunication sector and cyberspace, with the taking-control of TCI as its pinnacle, is now public knowledge and well-documented.⁹⁰ As a result of its control of TCI, the IRGC now has full control over the entire telephone and Internet network in Iran. This is due to the fact that TCI has a near monopoly on Iranian landline telephone services⁹¹, and reportedly all Internet traffic in and out of the country travels through TCI.⁹² This is particularly problematic since TCI purchased "a powerful surveillance system capable of monitoring landline, mobile and internet communications" from a Chinese firm in 2010.⁹³

In addition, according to an August 2013 article, all mobile phone operators in Iran are directly or indirectly partners with IRGC-affiliated companies.⁹⁴ This has been confirmed in a more recent report by Small Media (see Annex 4), which shows that all of the four mobile service providers in Iran have direct links to security or military organizations in Iran, with some of them under direct the ownership of the IRGC. They include:

1. **Mobile-Telecommunication Company of Iran (MCI – known locally as Hamrah-e Aval)**, which provides services to more than two-thirds of mobile subscribers in the Iranian telecoms market, is owned by TCI, and therefore it is assumed that IRGC enjoys a degree of access to customer data through its share in the company.⁹⁵
2. **Taliya**, which is jointly owned by a commercial arm of the IRGC known as *Bonyad*

⁹⁰ See for example: *ibid*; TeleGeography's GlobalComms Database, "Iran's TCI to merge fixed and mobile operations", 16 September 2016, available at: <https://www.telegeography.com/products/commsupdate/articles/2016/09/16/irans-tci-to-merge-fixed-and-mobile-operations> accessed 5 September 2017; *Digarban*, "The Revolutionary Guards is entering the IT market", December 12, 2011, available at: <http://www.digarban.com/node/3715>; also cited in Freedom House, "Iran Country Profile: Freedom of the Net 2016", available at: <https://freedomhouse.org/report/freedom-net/2016/iran>, at p. 4, accessed 5 September 2017.

⁹¹ Reuters, "Special Report: Chinese firm helps Iran spy on citizens", March 22, 2012, available at: <http://www.reuters.com/article/us-iran-telecoms/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSBRE82LOB820120322> accessed 5 September 2017.

⁹² Ian Black, "How Iran is filtering out dissent," *The Guardian* (UK), June 30, 2009, available at: <https://www.theguardian.com/technology/2009/jun/30/internet-censorship-iran> accessed 5 September 2017.

⁹³ Reuters, "Special Report: Chinese firm helps Iran spy on citizens", March 22, 2012, available at: <http://www.reuters.com/article/us-iran-telecoms/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSBRE82LOB820120322> accessed 5 September 2017.

⁹⁴ Khouroush Avaeei, "What to expect in Iran's Telecom Sector," *Al Monitor*, August 18, 2013, available at <http://www.al-monitor.com/pulse/originals/2013/08/expect-iran-telecom-sector.html> accessed 5 September 2017.

⁹⁵ According to the information published on MCN's website, it has over 18 million postpaid and over 47 million prepaid subscribers. As of the date of the present complaint, 90% of MCI's shares belong to TCI and 10% of shares are publicly traded at Tehran Stock Exchange. See: <https://www.mci.ir/web/en/aboutus> accessed 5 September 2017.

e Ta'avon, and Setad which, as stated above, belongs to the office of the Supreme Leader.⁹⁶

As documented in the report by Small Media (see Annex 4), the IRGC has a significant influence over the ICT sector in Iran, and the capabilities and tactics used by the IRGC demonstrate its intention to gain further control over all aspects of the sector. This means more serious breaches of fundamental rights of Iranian Internet users. Below are only few examples of the IRGC's capabilities and tactics:

- (1) **Computer and network surveillance:** Reuters revealed in 2012 that part of a \$130.6 million contract for networking equipment supplied by Shenzhen, China-based ZTE Corp, in 2010, TCI purchased a powerful surveillance system capable of monitoring landline, mobile and internet communications.⁹⁷
- (2) **Social networks monitoring and analysis:** The IRGC claimed in August 2016 that through monitoring and analyzing social network activities, it had arrested administrators of 450 channels and groups on WhatsApp, Telegram, and Instagram.⁹⁸
- (3) **Phishing:** A series of reports was published in April 2016 which showed that IRGC targets high-level politicians close to President Rouhani by sending fake login pages to them in order to discover their password and get access to their accounts.⁹⁹

As such, it is submitted that IRGC's authority, means and longstanding record in controlling telecommunications and the Internet in Iran cannot and should not go unnoticed in light of international provisions on human rights and principles establishing a corporate responsibility to respect them.

VI. BREACHES OF THE OECD GUIDELINES

Despite the exceptional severity and great predictability of adverse social and human rights impacts of the Italtel-TCI MoU, as explained above, Italtel has failed to disclose any information about whether and which risks and potential adverse impacts it is taking into account in designing the services and technologies it intends to provide to the TCI as per the MoU. Furthermore, the complainants are unaware of any measures taken by Italtel to identify, seek to prevent or mitigate the adverse impacts to which Italtel will inevitably risk to contribute by entering into an agreement with the TCI.

⁹⁶ ITNA, 'IRGC's Bonyad Ta'avon Purchased Talia' (in Farsi), 12 May 2012, available at: <<http://itna.ir/fa/doc/report/22145/اد-عاون-بن-یاد-خری-د-تالی-اس-پاه-ت-عاون-بن-یاد>> accessed 5 September 2017.

⁹⁷ Reuters, "Special Report: Chinese firm helps Iran spy on citizens", March 22, 2012, available at: <<http://www.reuters.com/article/us-iran-telecoms/special-report-chinese-firm-helps-iran-spy-on-citizens-idUSBRE82L0B820120322>> accessed 5 September 2017.

⁹⁸ Mehr News, 'Admins of 450 channels and groups of social media arrested by IRGC', 23 August 2016, available at: <<http://www.mehrnews.com/news/3750008/مدیران-۴۵%DB%B0-گروه-کمان-ال-و-گروه-دش-دند-د-دس-تگی-ر-س-پاه-ت-وس-ط-اجت-ماعی-های>> accessed 5 September 2017.

⁹⁹ See: International Campaign for Human Rights in Iran, "Revolutionary Guards' Cyber Attacks Now Directed at Rouhani Cabinet Members", available at: <<https://www.iranhumanrights.org/2016/04/cyber-attacks-iranian-officials/>> accessed 5 September 2017.

In the circumstances, the Complainants submit that Italtel has breached multiple principles of the OECD Guidelines, regardless of the extent of progress made so far by the parties to move forward with the Italtel-TCI MoU. This section sets out alleged breaches of the OECD Guidelines by Italtel in relation to the MoU reached in April 2016 between Italtel and TCI.

1. Failure to Conduct Risk-Based Human Rights Due Diligence

The complainants are unaware of any steps taken by Italtel to carry out a comprehensive human rights due diligence and to identify, prevent and account for the actual and potential adverse impacts of their entering into the MoU. Prior to engaging in negotiations for the provision of services, Italtel knew or should have known about Internet surveillance mechanisms and regulations in Iran and its impact on Iranian civil society and the Iranian population at large. Had Italtel conducted due diligence in accordance with an established responsible business conduct policy and had they carried out proper impact assessments it would have realized the gravity of the adverse impacts of its partnership with TCI and IRGC.

Even in the absence of a comprehensive human rights due diligence process, a basic assessment would have enabled Italtel to learn about TCI's role in censorship and violations of human rights and its association with the IRGC, and would have put Italtel on notice of the social risks of entering into the MoU.

As explained in section IV, Iran's deplorable human rights record is in the public domain and many reports by credible sources and ample information have been publicly available to Italtel about human rights violations in Iran. In relation to its record of human rights in general, and in relation to freedom of information and expression in particular, Iran has been a country of concern for many states as well as the EU and UN. Italtel knew, or should have known, the risks involved in entering into such an agreement. Italtel should have considered the severity of the adverse impact of their entering into an agreement with TCI and IRGC and cannot claim ignorance of the engagement of these entities in censorship and other human rights violations, nor can they claim they did not know about the role of IRGC in the telecom sector and TCI.

We therefore submit that Italtel has breached General Policies Chapter II, Paragraph A.10 and Human Rights Chapter IV, Paragraph 5.

Chapter II (General Policies)

A.10. “Enterprises should carry out risk-based due diligence, for example by incorporating it into their enterprise risk management systems, to identify, prevent and mitigate actual and potential adverse impacts as described in paragraphs 11 and 12, and account for how these impacts are addressed. The nature and extent of due diligence depend on the circumstances of a particular situation.”

Paragraph 14 of the Commentary on Chapter II also states:

“Due diligence is understood as the process through which enterprises can identify, prevent, mitigate and account for how they address their actual and potential adverse impacts as an integral part of business decision-making and risk management systems. Due diligence can be included within broader enterprise risk management systems, provided that it goes beyond simply identifying and managing material risks to the enterprise itself, to include the risks of adverse impacts related to matters covered by the Guidelines”

Chapter IV (Human Rights)

5. “Enterprises should carry out human rights due diligence as appropriate to their size, the nature and context of operations and the severity of the risks of adverse human rights impacts.”

Paragraph 45 of the Commentary on Chapter IV also states:

“Paragraph 5 recommends that enterprises carry out human rights due diligence. The process entails assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses as well as communicating how impacts are addressed. Human rights due diligence can be included within broader enterprise risk management systems provided that it goes beyond simply identifying and managing material risks to the enterprise itself to include the risks to rights-holders. It is an on-going exercise, recognizing that human rights risks may change over time as the enterprise’s operations and operating context evolve.”

2. Failure to Identify the Full Scope and Severity of Potential Adverse Human Rights Impacts

As explained above, many reports and ample information have been publicly available to Italtel about the role of IRGC and TCI in systematic breaches of human rights including the rights to freedom of information and expression. The scope of this information is such that any claim of lack of knowledge of these facts should be interpreted and dismissed as willful blindness, also taking into account Italtel's failure to respond to the Complainants' correspondences about such matters in the months preceding the filing of this complaint,

Italtel does not appear to have identified, or has failed to give any effect to, the full scope and severity of potential human rights impacts. There is an absence of a real and sustained effort or any indication of an intention to listen to and reflect upon the opinions and concerns of affected communities and human rights defenders. This is a clear breach of the Guidelines on the company's duty to assess the full scope and severity of potential human rights impacts.

Italtel knew or should have known about the long-lasting and extensive violations of human rights, including the right to privacy, in which the IRGC, as the main shareholder controlling the TCI, has been involved. Italtel has further failed to inquire into the relevant Internet surveillance policies currently in force in Iran, which form part of the enforcement measures for cyber crimes under Iranian legislation.

We therefore submit that Italtel has breached General Policies Chapter II, Paragraph A.11 and Human Rights Chapter IV, Paragraph 2.

Chapter II (General Policies)

A.11. "Avoid causing or contributing to adverse impacts on matters covered by the Guidelines, through their own activities, and address such impacts when they occur."

Chapter IV (Human Rights)

2. "Within the context of their own activities, avoid causing or contributing to adverse human rights impacts and address such impacts when they occur."

Paragraph 42 of the Commentary on Chapter IV also states:

"Paragraph 2 recommends that enterprises avoid causing or contributing to adverse human rights impacts through their own activities and address such impacts when they occur. 'Activities' can include both actions and omissions. Where an enterprise causes or may cause an adverse human rights impact, it should take the necessary steps to cease or prevent the impact. Where an enterprise contributes or may contribute to such an impact, it should take the necessary steps to cease or prevent its contribution and use its leverage to mitigate any remaining impact to the greatest extent possible. Leverage is considered to exist where the enterprise has the ability to effect change in the practices of an entity that cause adverse human rights impacts."

3. Failure to Disclose Information Including Social Reporting

Italtel has failed to provide sufficient information in relation to the content of the MoU and subsequent negotiations, including start date and the extent of Italtel's services and other business activities in Iran.

Section III of the Guidelines on Disclosure states that enterprises "should ensure that timely, regular, reliable and relevant information is disclosed regarding their activities, structure, financial situation and performance" and that "[e]nterprises are also encouraged to apply high quality standards for non-financial information including environmental and social reporting where they exist. The standards or policies under which both financial and non-financial information are compiled and published should be reported." In particular, Italtel has breached points 1, 2 and 4 (e) of this section.

Section III (Disclosure)

1. Enterprises should ensure that timely, regular, reliable and relevant information is disclosed regarding their activities, structure, financial situation and performance. This information should be disclosed for the enterprise as a whole and, where appropriate, along business lines or geographic areas.

2. Enterprises should apply high quality standards for disclosure, accounting, and audit. Enterprises are also encouraged to apply high quality standards for non-financial information including environmental and social reporting where they exist. The standards or policies under which both financial and non-financial information are compiled and published should be reported.

4. (e) Enterprises should also disclose material foreseeable risk factors.

Paragraph 28 of the Commentary on Chapter III also states:

“Clear and complete information on enterprises is important to a variety of users ranging from shareholders and the financial community to other constituencies such as workers, local communities, special interest groups, governments and society at large. To improve public understanding of enterprises and their interaction with society and the environment, enterprises should be transparent in their operations and responsive to the public’s increasingly sophisticated demands for information.”

4. Failure to Promote Internet Freedom through Respect of Freedom of Expression Online

By entering into the MoU, Italtel has entered into partnership with one of the main violators of Internet freedom and the freedom of expression in Iran. Italtel has moved in the complete opposite direction of what the OECD Guidelines require enterprises to do in relation to internet freedom and the rights to freedom of expression, assembly and association online.

We therefore submit that Italtel has breached General Policies Chapter II, Paragraph B.1.

Chapter II (General Policies)

B1. Duty to support cooperative efforts to promote Internet Freedom through respect of freedom of expression, assembly and association online.

5. Other Potential Breaches

In the event that the MoU results or has resulted in a binding contract and enters or has already entered into operative phase, which due to Italtel's failure to disclose information regarding its activities may well be the case, further breaches of the OECD Guidelines seem inevitable. Under a binding contract Italtel will be or is already obliged to perform its contractual duties and also to comply with the regulations set by the Islamic Republic authorities. This entails serious risks of complicity in human rights violations through contribution to the activities of the IRGC and TCI.

By entering into a binding contract with the TCI, while failing to comply with the above OECD Guidelines, Italtel will also fail to respect and avoid infringing upon a myriad of human rights protections, including, among other rights indicated herein, the freedom of expression and information, assembly and association, the right to privacy, freedom from torture and the right to life through inevitable complicity with IRGC and TCI.

We therefore submit that if Italtel enters, or has already entered, into an operative contract with TCI, it risks breaching General Policies Chapter II, Paragraph A.11 and A.12 and Human Rights Chapter IV, Paragraphs 1-4.

Chapter II (General Policies)

A.11. Avoid causing or contributing to adverse impacts on matters covered by the Guidelines, through their own activities, and address such impacts when they occur.

A.12. Seek to prevent or mitigate an adverse impact where they have not contributed to that impact, when the impact is nevertheless directly linked to their operations, products or services by a business relationship. This is not intended to shift responsibility from the entity causing an adverse impact to the enterprise with which it has a business relationship.

Chapter IV (Human Rights)

1. Respect human rights, which means they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.

2. Within the context of their own activities, avoid causing or contributing to adverse human rights impacts and address such impacts when they occur.

3. Seek ways to prevent or mitigate adverse human rights impacts that are directly linked to their business operations, products or services by a business relationship, even if they do not contribute to those impacts.

4. Have a policy commitment to respect human rights.

VII. OTHER RELEVANT INTERNATIONAL STANDARDS

Today, telecommunications and the Internet have become key means by which individuals can exercise their right to freedom of expression and information, as guaranteed by Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR) as well as the *Universal Declaration of Human Rights*.

Article 19 of the ICCPR provides that “[e]veryone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.”

Article 17.1 of the ICCPR provides that “[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.” Similarly, Article 8 of the European Convention on Human Rights recognizes the right to respect for private and family life, home and correspondence.

Of equal importance to this case, Articles 6 and 7 of the ICCPR prohibit against any person being “subjected to torture or to cruel, inhuman or degrading treatment or punishment” or arbitrarily deprived of her or his “inherent right to life”, and Article 9.1 guarantees the “right to liberty and security of person” and the right not to “be subjected to arbitrary arrest or detention.” Further, fair trial and due process rights in criminal and non-criminal proceedings are guaranteed under Articles 9, 13, 14 and 15 of the ICCPR.

In addition, according to the United Nations’ Guiding Principles on Business and Human Rights¹⁰⁰, a business enterprise’s responsibility to respect human rights exists independently of the States’ abilities and/or willingness to fulfill their own human rights obligations. As such, Article 11 of the UN Guiding Principles provides that business enterprises should “respect human rights” and “avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.”

Article 13 of the UN Guiding Principles provides that the responsibility to respect human rights requires business enterprises to “avoid causing *or contributing* to adverse human rights impacts through their own activities, and address such impacts when they occur” and to “seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.”

Article 15 of the Guiding Principles requires business enterprises to put in place “policies and processes appropriate to their size and circumstances” including, at a minimum, “a policy commitment to meet their responsibility to respect human rights; a human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights; and processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.”

The EU has also adopted significant policy documents and pieces of legislation with specific impacts on business and human rights. The main internal EU policy framework addressing implementation of the UN Guiding Principles is the 2011 Communication on “A renewed EU strategy 2011-14 for Corporate Social Responsibility”.¹⁰¹ In its communication, the Commission emphasizes that in order to fully meet their corporate social responsibility, enterprises should have in place a process to integrate social, environmental, ethical, human rights and consumer concerns into their business operations and core strategy in close collaboration with their stakeholders, with the aim of:

¹⁰⁰ U.N. Office of the High Commissioner of Human Rights, “Guiding Principles on Business and Human Rights” (2011), HR/PUB/11/04.

¹⁰¹ European Commission, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions: A renewed EU strategy 2011-14 for Corporate Social Responsibility, Brussels, 25.10.2011, COM (2011) 681, available at:

<[http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com\(2011\)0681_/com_com\(2011\)0681_en.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2011)0681_/com_com(2011)0681_en.pdf)> accessed 5 September 2017.

- Maximising the creation of shared value for their owners/shareholders and for other stakeholders and society at large;
- Identifying, preventing and mitigating their possible adverse impacts.¹⁰²

In 2012, the European Council also adopted a Strategic Framework on Human Rights and Democracy with an Action Plan for putting it into practice.¹⁰³ It places specific importance on implementation of the UN Guiding Principles. It is stipulated as the EU Commission’s responsibility to “ensure implementation to the Commission Communication on Corporate Social Responsibility, in particular by developing and disseminating human rights guidance for three business sectors including ICT. The EU Member States are also required by the OECD Common Approaches to implement the relevant adverse project-related human rights impacts.

VIII. REQUESTS TO THE NCP

Considering that (a) Italtel is an Italian company with its headquarters located in Milan, Italy, and (b) the alleged violations of the OECD Guidelines takes place in the Islamic Republic of Iran (“Iran”), a non-OECD state, this Complaint is submitted to the Italian NCP as the Complainants believe that the Italian NCP is best placed and has the authority to facilitate dialogue, investigate the facts, and make a determination in this case.

Given that the normal course of events would require Italtel to imminently begin implementing steps under the MoU with TCI, and given that this would significantly increase the likelihood of additional violations of the OECD Guidelines and potentially wide-ranging and significant violations of the human rights of ordinary Iranians, and taking into account the lack of disclosure in this regard, the Complainants strongly urge the Italian NCP to consider this submission on an urgent basis.

The complaint is not simply intended to prevent the Italtel-TCI MoU from moving forward. It is crucial that Internet development in every country benefits from the most updated technical and technological standards, but more importantly from fundamental international human rights standards, in order to maintain the Internet as a global space for free expression, communication, deliberation, development and economic expansion. A disconnect between the interests of advancing Internet and related technologies and the imperative of protecting human rights online can bear harmful consequences for communities and Internet users, and the value of technology.

As such, it merits recalling that the Complainants are not seeking to prevent Italtel’s potential business activities in Iran. Rather, they seek to ensure that:

¹⁰² Ibid, s 3.1.

¹⁰³ The EU “Strategic Framework on Human Rights and Democracy” is the main external policy framework in the area of human rights and its “Action Plan” was first adopted in June 2012 for the years 2012-2014. The current Action Plan on Human Rights and Democracy is adopted for the years 2015-2019, available at <https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/131181.pdf> accessed 5 September 2017.

- Italtel guarantees and uses its leverage to ensure that the technology transferred to Iran will not be used to facilitate any human rights violations;
- Italtel complies with the OECD Guidelines and the due diligence expectations of the Guidelines before Italtel starts operations in Iran; and
- Italtel adopts and implements a human rights and privacy rights policy to prevent complicity in violations of human rights, including privacy rights, by the government of Iran, and avoid adverse impacts on the Iranian civil society, youth and the population at large

As such, the Complainants call for an immediate moratorium on current negotiations between Italtel and TCI until such time that the aforementioned conditions are met and the actual and potential breaches to the Guidelines are recognized and effectively mitigated.

The Complainants acknowledge that, given the severe adverse impacts the community is experiencing, the NCP may wish to carry out a fact-finding mission to verify the facts.

The Complainants are at the full disposition of the NCP to provide further clarity or background information on any allegations or statements made, to facilitate access to witnesses or others who may wish to provide direct evidence on the matters referred to in this submission, or in any other way. The Complainants hope that this would allow a more expeditious and accurate verification of the facts alleged herein and a timely and just resolution of this Complaint.

We request the NCP to make an assessment of the facts and circumstances in a final statement, including whether the allegations contained herein constitute breaches of the Guidelines.

The Complainants further request the NCP to facilitate a constructive two-way dialogue between Italtel and the Complainants in order to address the above issues in a responsive and transparent way.

Given their in-depth knowledge and experience with local laws and practices in this area, the Complainants are prepared to assist Italtel, where necessary, in conducting a proper risk and impact assessment and elaborating a due diligence plan prior to engaging in further negotiations with the TCI, fully under the auspices of the Italian NCP.

In accordance with the procedural timelines set out by the Italian NCP for handling specific instances, a receipt confirmation should be provided to the Complainants within 7 days, and the result of the initial assessment within 30 days, of the reception of this Complaint or any additional documents required.

We look forward to a confirmation of receipt of this Complaint, and appreciate your assistance and leadership in resolving the issues raised herein.

We request that all correspondence in this matter be addressed to Ms. Shadi Sadr, Executive Director of Justice for Iran, at shadis@jfingo.org.

press release



**ITALTEL AND TCI AGREE TO COOPERATE ON
TELECOMMUNICATION DEVELOPMENT PROJECTS IN IRAN**

Teheran, 13 April 2016 – Italtel, a leading Italian telecommunications company in Network Functions Virtualization (NFV), managed services and all-IP communication, has entered into a Memorandum of Understanding (MoU) with Telecommunication Company of Iran (TCI) to develop and modernize TCI's telecom network.

The MoU was signed during an official Italian Government mission to Iran led by Italian Prime Minister Matteo Renzi.

Under the MoU, the parties have agreed to cooperate on the development of the Iranian telecommunications sector.

“The MoU signed today represents a fundamental step forward in the cooperation between Italy and Iran , said Stefano Pileri, Italtel CEO, and we are proud to be part of this important project. Telecommunications and ICT represent indeed an accelerator for the development of many other areas and economy in general”.

Having built up a wealth of experience in building and transforming complex networks of a large number of international operators, Italtel currently operates in the EMEA and LatAm markets, addressing Large Enterprises, Public Administration and Service Providers as a market leader in digital transformation.

Italtel

Italtel designs, develops, implements solutions for NGN and NGS; Professional Services dedicated to the design and maintenance of networks; IT System Integration Services; Network Integration and migration activities. Italtel counts among its customers more than 40 of the world's top TLC Operators and SPs. In Italy Italtel is also reference partner of Enterprises and Public Sector for the deployment of IP Next-Generation Networks and for the development of multimedia convergent services for their customers. Italtel is present in many countries including France, UK, Spain, Germany, Belgium, Poland, United Arab Emirates, Argentina, Brazil. www.italtel.com.

For more information

Italtel Communications

Laura Borlenghi

Tel.: +39 02 4388 5275

Mobile: +39 335 769 4240

E-mail: laura.borlenghi@italtel.com

Tiziana Rognoni

Tel.: +39 02 4388 5255

Mobile: +39 340 332 5553

E-mail: tiziana.rognoni@italtel.com

Annex 2: TCI's Press Release



April 17, 2016

TCI and Italtel signed an MoU to cooperate on telecommunication development projects in Iran

TCI signed cooperation MoU with Italtel to develop the country's telecom network.

The MoU was signed during an official Italian Government mission to Iran led by Italian Prime Minister Matteo Renzi in the presence of Iranian Foreign Affairs Minister Mohammad Javad Zarif.

According to the TCI PR and Int'l Affairs report, the ceremony was also attended by Dr. Seyed Hashemi, TCI chairman of the board, Mr. Dehnad, TCI acting CEO, Mr. Kargozar, TCI CEO Deputy and head of Technical and Commercial Operations Center and Stefano Pileri, Italtel CEO.

Under the MoU, the parties have agreed to cooperate on the development of the Iranian telecommunications sector, which is crucial for the country's economic development and the provisioning of new services in the education and healthcare sectors.

The MoU covers the IP-NOC, IP-BB projects as well as the development and renovation of NGN equipment and the new TCI value-added services with the world latest technology. Under the MoU, Italtel is committed to provide the equipment and implement the Iranian telecom network on the basis of the plans designated by TCI within 18 months.

After signing the MoU, TCI acting CEO said: " TCI is the largest telecom company in the Middle East region with the vast potential for investment. "

Stressing on the fact that our strategy is the expansion of investment, Mr. Dehnad stated:" In addition to quantity and quality expansion of TCI, we seek to employ this capacity for the prosperity of the national economy."

He added: "To achieve the country's telecom development goals, we are willing to make good use of the interested countries' capacities, including Italy."

“The MoU signed today represents a fundamental step forward in the cooperation between Italy and Iran and we are proud to be part of this important project. Telecommunications and ICT represent indeed an accelerator for the development of many other areas and economy in general”, said Stefano Pileri, Italtel CEO.

He further added: “Having built up a wealth of experience in building and transforming complex networks of a large number of international operators, Italtel currently operates in the EMEA and LatAm markets, addressing Large Enterprises, Public Administration and Service Providers as a market leader in digital transformation.”

It is worth mentioning that Italtel is a leading Italian telecommunications company in Network Functions Virtualization (NFV), managed services and all-IP communication.

REDRESS

Ending Torture, Seeking Justice for Survivors

April 12, 2017

Italtel Group SpA

c/o Mr. Stefano Pileri, CEO

Via Reiss Romoli - loc. Castelletto

20019 Settimo Milanese

Milano, Italy

Email: stefano.pileri@italtel.com

CC'd: laura.borlenghi@italtel.com; tiziana.rognoni@italtel.com

"By Email and Regular Mail"

Subject: Italtel-TCI Memorandum of Understanding of April 13, 2016

Dear Sir,

REDRESS is an international human rights organization with a mandate to seek justice and other remedies for victims of torture. Justice for Iran is a non-governmental organization based in the UK aiming to address impunity and seek accountability for human right violations in Iran. Further information on our respective organizations are available on our websites: www.redress.org and www.justiceforiran.org.

We are writing to inquire about the Memorandum of Understanding (MoU) that was reached between Italtel S.p.A. and the Telecommunication Company of Iran (TCI) on April 13th, 2016, as per a press release published on your company's website on the same date.¹ Under the MoU, Italtel and TCI would have "agreed to

¹ <http://www.italtel.com/content/uploads/2016/04/PR-Italtel-Iran.pdf>

REDRESS LONDON

87 Vauxhall Walk, London SE11 5HJ

Tel: +44 (0)20 7793 1777 Fax: +44 (0)20 7793 1719

Email: info@redress.org

Registered Charity N. 1015787

A Limited Company Registered in England Number 2274071

REDRESS NEDERLAND

Laan van Meerdervoort 70, 5th floor; Rm 5.04

2517 AN, Den Haag, The Netherlands

Tel: +31 708 919 317

Email: info.nederland@redress.org

Registered with the Chamber of Commerce, file number 66793319

PATRONS

Justice Louise Arbour CC, GOQ
Professor Michael Bazylar (USA)
Professor Theo van Boven (The Netherlands)
Rt Hon Ann Clwyd MP
Lord Crickhowell
Dato' Param Cumaraswamy (Malaysia)
Edward Datnow FRCS
Anthony Foulger
Dr Inge Genefke MD, D.M.Sc.h.c.(DK)
Earl of Haddington
Lord Harries of Pentregarth
Dame Rosalyn Higgins DBE QC
Lord Judd
Lord Lester of Herne Hill QC
Caroline Moorehead OBE, FRSL
Professor Manfred Nowak (Austria)
Sir Nigel Rodley KBE
John Simpson CBE
Professor David Weissbrodt (USA)
Dame Vivienne Westwood DBE

TRUSTEES (LONDON)

Paul Lomas (Chair)
Michael Birnbaum QC
Professor Bill Bowring
Sherman Carroll Ph.D, MBE
Willa Maria Geertsema
Frances Mary Guy
Jasvir Kaur
Leah Levin OBE
Rev. Nicholas Mercer
Nimisha Patel
Baroness Vivien Stern

TRUSTEES (NEDERLAND)

Paul Lomas (Chair)
Willa Maria Geertsema
Rianne Letschert


LEGAL ADVISORY COUNCIL

Professor Michael Bazylar
Sir Geoffrey Bindman QC (Hon)
Joanna Glynn QC
Professor David Harris CMG
Professor Lorna McGregor
Professor Geraldine Van Bueren
Professor David Weissbrodt

FOUNDER

Keith Carmichael

WWW.REDRESS.ORG



cooperate on the development of the Iranian telecommunications sector". However, limited information has thus far been made available regarding the specific services and/or products covered under the aforementioned MoU.

Given the widespread and well-documented human rights abuses perpetrated by Iran and facilitated by the telecommunications industry in the country, we would hope that the company has taken appropriate steps to consider whether there may be any human rights implications about the proposed cooperation detailed above.

Therefore, we would be grateful to receive further information about the steps you may have taken to ascertain those risks and to mitigate them, as appropriate. We would also welcome to receive a copy, or relevant provisions of the MoU describing the services and/or products to be supplied to the TCI, or, further general information regarding:

- (i) the services and/or products contemplated under the MoU;
- (ii) whether and how Italtel has conducted any assessment of the risks and potential adverse impacts of its specific business activities in Iran, both prior to engaging in negotiations with the TCI and in designing the services and/or products it intends to provide to the TCI as per the MoU;
- (iii) whether and how Italtel has, or intends to, put in place an adequate and comprehensive human rights due diligence plan, prior to engaging in further negotiations with the TCI;
- (iv) whether and to what extent the MoU has led to a binding and operative contract; and
- (v) what services and/or products have already been delivered to the TCI.

We are at your full disposal to discuss our interest in this matter and to provide any further information that you may require. We thank you in advance for your transparency and collaboration in this regard.

Sincerely,



Carla Ferstman
Director

REDRESS

Ending Torture, Seeking Justice for Survivors

23 May 2017

Italtel Group SpA

c/o Mr. Stefano Pileri, CEO

Via Reiss Romoli - loc. Castelletto

20019 Settimo Milanese

Milano, Italy

Email: stefano.pileri@italtel.com

CC'd: laura.borlenghi@italtel.com; tiziana.rognoni@italtel.com

"By Email and Regular Mail"

Subject: Italtel-TCI Memorandum of Understanding of April 13, 2016

Dear Sir,

We wrote to you on 12 April and unfortunately have not received a reply. For your convenience, we attach a duplicate of that letter.

As indicated in that correspondence, we would welcome the opportunity to discuss with the Italtel Group its various activities in Iran.

We would remind that in accordance with the applicable OECD principles, as well as the operable legal framework concerning support and provision of services in Iran, there is an obligation for Italtel to report fully on its activities and to assess the social impact of its work and carry out on an ongoing basis human rights due diligence. We are unaware of the steps that Italtel has taken in this regard and would welcome your response.

Thank you for your attention to this matter. I can be reached at the above coordinates or by email at: carla@redress.org.

Sincerely,

Carla Ferstman
Director

PATRONS

Justice Louise Arbour CC, GOQ
Professor Michael Bazzyler (USA)
Professor Theo van Boven (The Netherlands)
Rt Hon Ann Clwyd MP
Lord Crickhowell
Dato' Param Cumaraswamy (Malaysia)
Edward Datnow FRCS
Anthony Foulger
Dr Inge Genefke MD, D.M.Sc.h.c.(DK)
Lord Harries of Pentregarth
Dame Rosalyn Higgins DBE QC
Lord Judd
Lord Lester of Herne Hill QC
Caroline Moorehead OBE, FRSL
Professor Manfred Nowak (Austria)
John Simpson CBE
Professor David Weissbrodt (USA)
Dame Vivienne Westwood DBE

TRUSTEES (LONDON)

Paul Lomas (Chair)
Michael Birnbaum QC
Professor Bill Bowring
Sherman Carroll Ph.D, MBE
Willa Maria Geertsema
Leah Levin OBE
Rev. Nicholas Mercer
Baroness Vivien Stern

TRUSTEES (NEDERLAND)

Paul Lomas (Chair)
Willa Maria Geertsema
Rianne Letschert

LEGAL ADVISORY COUNCIL

Professor Michael Bazzyler
Sir Geoffrey Bindman QC (Hon)
Joanna Glynn QC
Professor David Harris CMG
Professor Lorna McGregor
Professor Geraldine Van Bueren
Professor David Weissbrodt

FOUNDER

Keith Carmichael

WWW.REDRRESS.ORG

REDRESS LONDON

87 Vauxhall Walk, London SE11 5HJ

Tel: +44 (0)20 7793 1777 Fax: +44 (0)20 7793 1719

Email: info@redress.org

Registered Charity N. 1015787

A Limited Company Registered in England Number 2274071

REDRESS NEDERLAND

Laan van Meerdervoort 70, 5th floor; Rm 5.04

2517 AN, Den Haag, The Netherland

Tel: +31 708 919 317

Email: info.nederland@redress.org

Registered with the Chamber of Commerce, file number 66793319



MARCH 2017



Filterwatch



Iranian Internet Infrastructure and Policy Report

A *Small Media* monthly report bringing you all the latest news on internet policy and online censorship direct from Iran.

smallmedia.org.uk



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

— Executive Summary —

The last decade has seen increasing speculation about the growing role of the Islamic Revolutionary Guard Corps (IRGC) in the imposition of information controls on Iranian citizens. This month's feature provides an overview of the various ways in which the IRGC has been able to regulate and otherwise affect the flow of information in online spaces, and shares a number of case studies documented by [Justice for Iran](#) demonstrating IRGC-directed information controls in action.

Also this month, we continue to review the major developments in internet policy from March 2017. Iran's National Information Network (SHOMA) saw further progress, with the Communications Regulatory Authority (CRA) ordering providers to divide users' bills based on their use of domestic and international content. Customers accessing domestic content will see a 50% cut to their internet tariffs – a clear move by Iran to entice users away from international content and services by increasing accessibility to domestic services. In addition, the government announced that more than 5,500 Telegram admins had registered their details on the online registration system [Samandehi](#). Mid-way through the month, twelve such admins were [arrested](#), suggesting that the ulterior motives many feared about Telegram registrations were grounded in truth – the system empowers authorities to identify and detain users with ease.

Reports circulated on social media in March that the ICT Ministry has been in negotiations with Telegram, apparently offering them 800 billion IRR (24.6 million USD) to relocate their servers to Iran. Although ICT Minister Mahmood Vaezi denied the allegations, the resilience of these accusations speaks to the level of public unease about the nature of the relationship between Iran and Telegram.

Key Statements

- MARCH 5** ● The Director of the Center for Digital Media and Information Technology (**SARAMAD**) Seyed Morteza Mousavian announced that half of the Telegram administrators of channels with more than 5,000 users have registered their details with **Samandehi**, following orders from the Supreme Council of Cyberspace (SCC). According to Mousavian, 5,500 channels have registered their details. ([Source](#))
- MARCH 12** ● ICT Minister Mahmoud Vaezi denied reports that Telegram would be replaced with an Iranian version of the app, claiming there were no plans to do so. In other comments he said that social media platforms will play a key role during the upcoming election campaign, stating that they were useful tools to help Iranians make their decision. ([Source](#))
- MARCH 15** ● Saeed Reza Ameli, a member of the Supreme Council of Cyberspace (SCC), said 76% of Iranians use circumvention tools. He said this demonstrated the need for citizens to be more educated about cyberspace, and the necessity of producing more religious content. ([Source](#))
- MARCH 21** ● ICT Minister Mahmoud Vaezi said telecommunications will be improved in preparation for the upcoming presidential and local council elections. He added that the number of internet users has increased from 200,000 to 40 million and he also promised that 90% of villages in Iran will have access to online services by the end of the current government. ([Source](#))
- MARCH 25** ● The ICT Minister denied reports that the government is negotiating with Telegram and offering to pay the company 800 billion IRR (24.6 million USD) to relocate their servers to Iran. ([Source](#))

1

The Islamic Revolutionary Guard Corps and Information Controls

Over the last decade, the Islamic Revolutionary Guard Corps (IRGC) has rapidly expanded its control over Iran's ICT sector. In turn, this has led to growing speculation about the role the IRGC plays in imposing information controls on Iranian internet users.

Information controls are designed to limit the freedom of internet users in Iran and maintain the Iranian government's control over all aspects of the internet in the country.

The IRGC is officially represented in a number of internet policy making bodies in Iran, but some of their actions in recent years have suggested that they may have the capacity to threaten internet freedom from outside these official channels. In recent years there have been a number of occasions in which the IRGC has publicised their arrest of Iranian citizens based on their online activities. For example, on [November 7 2015](#), the IRGC in Qazvin province arrested the admins of over 170 active social network groups and channels after a "technical and intelligence" operation. The IRGC claimed that the groups were publishing "immoral" content online.

Alongside these high profile IRGC announcements, [Justice for Iran](#) reports that it has received information from a number of individuals describing the IRGC's role in waging cyberattacks. Victims report that the IRGC has engaged in attacks to uncover personal information, identify them via their online activities, or pinpoint their location via their mobile phones. Taking together the widely publicised reports of IRGC-led arrests, and the accounts of those targeted by the IRGC, we believe it is important to ask searching questions about the IRGC's ability to monitor and obstruct the online activities of Iranian users.

This report will begin to gauge the IRGC's reach and influence online by highlighting their control over key points of Iranian ICT infrastructure, and examining their role in influencing ICT policy development and implementation. This report also covers a series of case studies demonstrating how the IRGC has made use of this control over ICT infrastructure to arrest or prosecute individuals inside Iran.

We would note that this report only highlights the aspects of the IRGC's activities that have been publicly identified – additional information control capacities may exist, and further investigations are required. Nonetheless, this report demonstrates that the IRGC's capabilities to impose and implement information controls in Iran should be of immense concern to anyone interested in internet freedom and human rights in Iran.

THE IRGC AND THE ICT SECTOR IN IRAN

The IRGC was established to defend the revolutionary values of the 1979 Iranian Revolution. Paranoid about the potentially divided loyalties of the Iranian military, Ayatollah Sayyid Ruhollah Khomeini established the IRGC in 1979 to protect the Revolution against political rivals and competing ideological strands within the revolutionary coalition. During the immediate post-revolutionary period, the IRGC worked with the vestiges of the Pahlavi-era intelligence services to crush opposition groups such as the communist Tudeh party and the militant Mujahedin-e Khalq, and consolidate state power with the clerical establishment.

The IRGC's influence continued to grow in the years following the Revolution. During the long Iran-Iraq War, the IRGC repeatedly clashed with the Iranian military about the tactics employed on the battlefield. More recently, the IRGC have been involved in combating domestic and regional uprisings, including in the Kurdish regions of Iran and the Syrian Civil War.

Another defining feature of the IRGC is their growing economic power. Through holding companies and charitable trusts the IRGC has developed a **financial network worth billions of dollars**. In addition to this, during the period that Iran was under heavy international sanctions due to its nuclear programme, the **IRGC grew substantially** through affiliated entities such as the Khatam-al Anbiya Construction Headquarters, through which it won a number of government construction contracts. This financial expansion has developed out of the IRGC's political ideology, which is premised upon independence from the government in order to safeguard the Islamic Revolution from ideological divergence.

The IRGC's involvement in the ICT sector is in line with its objective to defend the Islamic Republic from any ideological or political threats, and to remain economically independent by entrenching itself in the private and public sectors.

In recent years the IRGC has managed to expand and consolidate its influence on the internet in Iran through their control over the telecommunications sector, their political influence – through formal and informal legal and policy processes – and through extra-legal cyberattacks. Furthermore, Supreme Leader Ali Khamenei's development of the discourse around 'Soft War' by has been used by the IRGC to create a culture of fear and self-censorship among Iranian internet users.

THE IRGC'S INFLUENCE ON IRANIAN ICT INFRASTRUCTURE

The Telecommunication Company of Iran (TCI) was established as a state-owned telecommunications company in 1971, and for many years was the sole investor in Iran's ICT sector, and the only provider of landline phone services to Iranians. However, as a result of a direct order from the Supreme Leader in 2006, the TCI was named as one of the national industries slated for privatisation.

In 2009, President Mahmoud Ahmadinejad put 50%+1 of TCI's shares on sale at auction. At the end of the auction, Tose'e Etamad Mobin (TEM) consortium was announced the new majority shareholder of the TCI. The consortium was newly formed, and the three companies that were in it were either owned by the IRGC or by Setad, both of which operate under direct command of the Supreme Leader. This was a source of controversy, as a number of other companies claimed their bid was not received by Ahmadinejad's government, and that the auction was fixed in favour of TEM.

The privatisation process by which the IRGC and Setad became the common majority shareholder of TCI remains controversial in Iran, and despite a recent call for re-auctioning the shares awarded to TEM the consortium remains majority shareholders.

Case Study

An ordinary citizen was contacted by intelligence services, who asked her to come for a briefing. Although she told the services that she is not in Iran, they said they knew she was in the country and that she must stop using a specific website, or else the intelligence services would come after her and charge her for collaboration with terrorists.

The Role of ICT

As all SIM cards must be registered under the name of their owner, the intelligence services could access her details and pinpoint her via telecommunication towers. Iranians have previously encountered challenges around mobile phone surveillance, when the prominent journalist Issa Saharkhiz [sued](#) Nokia Siemens Networks for selling Iran tools to monitor mobile phone conversations.

Risks

The intelligence services, including the IRGC, have the power to pinpoint dissidents' locations if they turn on their phones inside Iran – even if their devices are not smartphones. As the IRGC is the owner of the TCI, they can pinpoint the location of the target without obtaining judicial permission.

In Iran there are currently four mobile phone service providers: the Mobile Telecommunication Company of Iran (MCI), MTN Irancell, RighTel, and Taliya. All four of these mobile service providers in Iran have direct links to security or military organisations in Iran, with some of them under direct ownership of the IRGC:

- MCI remains the most popular service provider, and it is owned by the TCI. It is therefore assumed that the IRGC enjoys some degree of access to customers' data through its commercial share in the company.
- MTN Irancell is 49% owned by South African based MTN Group and 51% owned by Iran Electronics Industries – a subsidiary of the Ministry of Defence and Armed Forces Logistics.

- RighTel is owned by the Social Security Organization, which has a number of joint investments with the IRGC.
- Taliya is **jointly owned** by the IRGC's commercial company, and Setad, which belongs to the office of the Supreme Leader.

The IRGC's control of the TCI and other mobile phone service providers gives them influence over some of the ICT sector's most critical infrastructure. As a result, the IRGC has direct access to a broad section of Iran's ICT infrastructure, including unfettered access to the data of millions of internet users.

Case Study

A political activist was arrested by the IRGC and his phone was intercepted. According to this activist, he was part of a group that were arrested together, but none of them knew each other. The activist is sure his phone call was listened to by the IRGC because he tried to call his mother at the same time as the IRGC planned to arrest him, and his mother's voice was disrupted.

The Role of ICT

It is possible that the IRGC tapped his phone and listened to his conversations. As the IRGC controls 50%+1 of shares in the TCI, phone tapping is technically uncomplicated, and does not require judicial oversight.

Risks

As the IRGC is the main shareholder in many ICT companies, including the TCI, MCI and Taliya, it possesses sweeping powers to intercept communications via phone calls or SMS.

The IRGC's influence on mobile phone service providers is becoming more significant as more Iranians get online and try to connect to the internet via their mobile phones. For instance, Iran has more than 20 million users on Telegram, which is a valuable target for the IRGC.

Case Study

A political activist was interviewed by the IRGC, where he was presented with copies of his emails. His email account was hacked months before, despite the fact that he had activated two-step verification by text message on his account.

The Role of ICT

As the activist had enabled two-step SMS verification on his email account, the IRGC could obtain his password via a phishing attack – which is popular amongst Iranian hackers – and then hijack the two-step verification code by asking the mobile phone service providers to intercept the communication to obtain the code.

Risks

As the IRGC is the main shareholder in many ICT companies such as the TCI, MCI and Taliya, it has the power to intercept any communication via phone call or SMS. This power allows the IRGC to bypass some important security features such as SMS-based two-step verification.

THE IRGC'S INSTITUTIONAL INFLUENCE

The IRGC's participation in Iranian public life has always exceeded their military strength. With regard to the ICT sector and internet policy of the Islamic Republic of Iran, the IRGC possesses institutional influence within policy making bodies, security organisations and cultural and scientific institutes.

Iranian censorship and internet policy are formulated and directed by a number of official bodies in which the IRGC has played an influential role. The IRGC is often officially represented in bodies formulating internet policy in Iran, however on the occasions that they are not, they have used their public platform to influence decisions. The IRGC also has developed a number of organisations which seek to monitor and police cyberspace in Iran outside of the official bodies responsible for this task. There are two state organisations that the IRGC could use to influence internet policy:

- **The Supreme Council of Cyberspace (SCC):** One of the seats on the SCC is reserved for the Chief Commander of the IRGC (currently Major General Mohammad Ali Jafari).¹ This gives the IRGC influence in the development of national and international policy regarding cyberspace, although it must be noted that currently the majority of SCC seats are occupied by individuals aligned with President Hassan Rouhani's administration.
- **The Commission to Determine the Instances of Criminal Content (CDICC):** The IRGC is not represented on the CDICC, although in the past the IRGC has sought to influence the organisation. This was most notable during the debate on the filtering of Telegram. IRGC officials, the paramilitary volunteer militia the Basij and Gerdab, the propaganda arm of the IRGC on the internet, sought to **make the case against Telegram** in public to put pressure on the CDICC.

¹ The EU has adopted restrictive measures such as sanctions against General Jafari due to his role in serious human rights abuses. The Council of Europe reasoned its decision by saying: "IRGC and the Sarollah Base commanded by General Jafari has played a key role in illegally interfering with the 2009 Presidential Elections, arresting and detaining political activists, as well as clashing with protesters in the streets."

The IRGC has also sought to establish its own organisations to influence internet policy, which act in parallel to policy making and law enforcement bodies in Iran:

- ◇ **The IRGC's Intelligence Organisation:** It was established in 2009, and its main role is to participate in the online 'Soft War' and to identify digital threats to the Islamic Republic.
- ◇ **The Center for Inspecting Organised Crimes (CIOOC):** It was set up in 2007 and at the time its main task was to fight crimes such as money laundry and online theft. However, in the recent years it has taken part in the IRGC's effort to mentor and fight "moral" and political offenses online.²

Cultural and scientific activities are also part of the IRGC's strategy to enhance their influence online. This involves establishing or supporting educational, cultural, or commercial entities in Iran, which work directly with the internet and new technologists in the country. The IRGC's activities and influences in this area are much less visible and formal, and therefore harder to assess.

For example, the Imam Hossein Comprehensive University (IHCU), which is based in Tehran, is officially affiliated with the IRGC and it is known for training IRGC managers and officers in a range of subjects. The Department of Computer Science at the IHCU appears to be active in providing forums and conferences for scientists around Iran in studying and discussing different topics around digital security. For instance the IHCU, in association with the IRGC, holds an annual conference on [International Security and Cryptography](#), which attracts computer scientists and other academics from across the country.

² The CIOOC is on the list of the US human rights sanctions, adopted by the US Treasury. The order says: "The CIOOC has taken an active role in identifying and arresting protesters involved in the 2009 post-election unrest, particularly those individuals active in cyberspace. The CIOOC uses extensive methods to identify Internet users, including through an identification of their Internet Protocol (IP) addresses. The Iranian regime has identified and arrested many bloggers and activists through the use of advanced monitoring systems, and the CIOOC inspects forwarded emails to identify those critical of the regime."

THE IRGC AND THE 'SOFT WAR'

In the wake of the protests that followed the disputed presidential election in 2009, the Supreme Leader initiated the concept of "Soft War" in his public statements. By "Soft War" he refers to what he views as attempts by Western powers to influence Iran's culture through the media and the internet. The rhetoric around Soft War quickly became code for attacking internet freedom in Iran. This rhetoric was strongly echoed by IRGC officials and became the justification for a range of restrictive measures and aggressive rhetoric against internet freedom.

In the past IRGC officials have used their Soft War rhetoric to warn other officials and policy makers in Iran that all sections of the Iranian government must adopt a **hard-line policy** towards the enemy on cyberspace. This aggressive rhetoric from the IRGC has led to a culture of fear among Iranian internet users.

THE IRGC'S KNOWN TACTICS AND CAPABILITIES

The IRGC holds a lot of influence over the Iranian ICT sector owing to its broad financial and political powers. As a result, it is impossible to fully map out the IRGC's capabilities and tactics. The capabilities and tactics outlined below likely only cover a limited range of the IRGC's full repertoire, but they indicate the IRGC's intention to use their influence on the ICT sector to limit privacy and the human rights of Iranian internet users:

- **Computer and network surveillance:** Reuters **revealed** in 2012 that as part of a \$130.6 million contract for networking equipment supplied by Shenzhen, China-based ZTE, the TCI has purchased a powerful surveillance system capable of monitoring landline, mobile and internet communications,
- **Social network monitoring and analysis:** The IRGC claimed in **August 2016** that through monitoring and analysing social network activities, it has arrested administrators of 450 channels and groups on WhatsApp, Telegram, and Instagram.
- **Phishing:** A series of reports were published in **April 2016** that the IRGC targets high-level politicians close to President Rouhani by sending fake login pages to them in order to discover their password and gain access to their accounts.

- **IRGC's VPNs:** The vast majority of Iranians use VPNs for their daily internet use to bypass internet censorship in Iran. Although this has not been confirmed, some analysts believe that some of the VPNs sold to Iranians to circumvent censorship are actually **owned by the IRGC**. One of the reason for this belief is that many VPN sellers in Iran allow users to pay the subscription fee via official payment systems, even though selling VPNs is illegal under **Iran's Cyber Crime Law**.

CONCLUSION

Over the last decade the IRGC has expanded its control and influence over Iranian internet policy and ICT infrastructure. This rapid expansion was achieved using an array of commercial, institutional, cultural instruments. What is clear is that the IRGC has been using this influence to expand their surveillance capabilities, create a culture of of fear among internet users in Iran, and to crackdown on activists, journalists and ordinary citizens.

The level of control that the IRGC has gained in recent years is significant, and has allowed the organisation to identify, detain, and prosecute Iranian citizens on the basis of their online activities. As a result, it should be noted that although the internet has opened up innumerable opportunities for Iranians to express themselves, it has also made it easier for the IRGC to crack down on dissidents.

2

Content Filtering, Information Controls and Law Enforcement

- **March 1:** Head of Iran's Cyber Police (FATA) Seyed Kamal Hadianfar said cybercrime in Iran has increased by around 63%. He added that FATA's discovery rate of cybercrime is 88%, which he described as being 50% higher than the global average. It is unclear how FATA came to these statistics. ([Source](#))
- **March 7:** The Secretary of the Committee to Determine Instances of Criminal Content (CDICC) Abdolsamad Khoramabadi announced the Waze navigation app has been filtered. ([Source](#))
- **March 7:** Mohammad Jafar Montazari, Attorney-General of Iran said that Iran's judiciary blocks between 16,000 and 20,000 Telegram channels each week. He pointed that this amount of filtering is not enough and there must be more control over Telegram channels and therefore Iran needs to complete and use the National Information Network or SHOMA. ([Source](#))

3

Statements from Ministries and Politicians

- **March 1:** Vice President of the Communications Regulatory Authority (CRA) Sadegh Abbasi Shahkoo announced that two new licences have been issued for Mobile Virtual Network Operators (MVNO). ([Source](#))
- **March 1:** Minister of Justice Mostafa Pourmohammadi said Iran should have the power to regulate online activities, but this does not mean Iran has to miss out on the opportunities inherent to the internet. ([Source](#))
- **March 1:** ICT Minister Mahmoud Vaezi said that whilst some members of Iran's Parliament had asked for an increase in mobile and internet tariffs, the ICT Ministry will not increase them in the next year (March 2017 – March 2018). ([Source](#))
- **March 3:** Deputy Minister of ICT Ali Asghar Amidian said that in order to encourage the use of domestic contents, his ministry is going to decrease tariffs for internet bandwidth usage under 100 Mbps. ([Source](#))
- **March 4:** Hossein Fallah Joshaghani, Deputy of the Communications Regulatory Authority (CRA), said that operators have been ordered to divide users' bills based on content usage, so those using domestic content get charged less. This is a key part of the National Information Network (SHOMA), in that the government wants to separate domestic and international traffic for Iranians. Operators are also required to send users text messages before charging them for their services. ([Source](#))
- **March 5:** Mohammad Khansari, Head of the Iran Telecommunication Research Center (ITRC) announced the ITRC has prepared a roadmap for a 5G network in Iran. He also said that the infrastructure for national search engines is ready, and that Iranians are becoming more interested in this project. ([Source I](#), [Source II](#))
- **March 5:** Ali Asghar Amidian, Director of the Communications Regulatory Authority (CRA) said that the division of domestic from international traffic has been delayed by operators due to a lack

of infrastructure and preparations. He noted operators have three months from 5 March 2017 to notify users on their usage of domestic content and provide 50% off on their bills. ([Source](#))

- **March 5:** The Commission of Science and IT in the Supreme Cultural Revolution Council (SCRC) has reviewed a plan for the Internet of Things (IoT) and looked at its potential for the business and the society, as well as its impact on citizens' lives. ([Source](#))
- **March 5:** The Director of the Center for Digital Media and Information Technology ([SARAMAD](#)) Seyed Morteza Mousavian announced that half of the Telegram administrators of channels with more than 5,000 users have registered their details with [Samandehi](#), following orders from the Supreme Council of Cyberspace (SCC). According to Mousavian, 5,500 channels have registered their details. ([Source](#))
- **March 5:** Seyed Abolhasan Firouzabadi, Secretary of the Supreme Council of Cyberspace (SCC) said no messaging apps have been forced to obtain a licence. However, he claimed that the SCC would provide incentives for apps to apply for licences. He also asserted that if non-Iranian messaging apps were to receive licences, the SCC would guarantee that the app works without issue. ([Source](#))
- **March 5:** Deputy Minister of ICT Mohammad Javad Azari Jahroumi said that the number of mobile internet users has increased by up to 40 million since 2013. Jahromi also noted that the rate of brain drain has decreased since launching the National Information Network (SHOMA). He also said they hope each year they can create 100,000 new jobs in the ICT sector. ([Source](#))
- **March 6:** Iranian MPs have agreed a new budget for the Ministry of ICT that could help create new jobs in the ICT sector. Parliament has agreed to allocate 1.4 trillion IRR (1.7 billion USD) to the ICT Ministry. ([Source](#))
- **March 7:** ICT Minister Mahmoud Vaezi said that thanks to a collaboration with foreign and domestic companies, 8 cities in Iran will be equipped with fiber optic cables. The completion date of this project is not clear. ([Source](#))
- **March 7:** ICT Minister Mahmoud Vaezi, in response to the filtering of [Waze](#), said the main reason for filtering the app was because it was created by Israel. He added that Iran has already developed a replacement for the app. Vaezi said the blocking of the app took place through a court order. In another comment Vaezi said that 65% of projects relating to the 'Resistance Economy' project have been completed. Details of these projects are not clear. ([Source](#))

- **March 7:** Deputy Minister of ICT Mohammad Javad Azari Jahromi said Iran is improving self-sufficiency by producing fiber optic cables domestically. He also mentioned that with Iran investing 14 trillion IRR (17 Billions USD) in the fiber optic industry, it has managed to use domestic fiber optic for the fiber optic networks between Iran, Afghanistan and Iraq. This is an example of the 'Resistance Economy' program in the ICT sector in Iran. ([Source](#))
- **March 8:** Deputy Minister of ICT Mohammad Javad Azari Jahromi said the Communications Regulatory Authority (CRA) has agreed to decrease the bandwidth tariff by up to 20% for those who use the traffic on the National Information Network (SHOMA). ([Source](#))
- **March 8:** Vahid Sadoughi, director of the [Mobile Telecommunication Company](#) (MCI) said they have managed to receive compensation from a foreign company who stopped working with Iran during the sanctions but after the lifting of sanctions the company asked to re-enter the Iranian market. Sadoughi said that the MCI have received 500 million EUR but did not name the company. ([Source](#))
- **March 8:** Secretary of the Supreme Council of Cyberspace (SCC) Seyed Abolhasan Firouzabadi said the recent filtering of [Waze](#) was the result of a court order, and not a decision of the Committee to Determine Instances of Criminal Content (CDICC). ([Source](#))
- **March 10:** Seyed Reza Salehi Amiri, Minister of Culture and Islamic Guidance (MCI), said that Iran should not look at social media as a threat, but rather as an opportunity. He asserted that to stop 40 million Iranians from using social media would be impossible. ([Source](#))
- **March 11:** ICT Minister Mahmoud Vaezi said everyone in Iran will have access to 3G networks, and that more than 750 cities will have access to the 4G network by the end of Rouhani's government in May 2017. In another comment about the blocking of Waze, Vaezi said there are other non-Iranian apps that users can use. He had previously suggested that there are lots of other Iranian apps that can replace Waze. Vaezi also said members of the Supreme Council of Cyberspace (SCC) have discussed different options for regulating the app Clash of Clans but no decision has been made, meaning the application is still available to Iranians. ([Source](#))
- **March 11:** Deputy ICT Minister Mohammad Javad Azari Jahromi said that internet tariffs have noticeably decreased since 2013. The price for 1 Gbps in Tehran in 2013 was 36,000 IRR (1.11 USD) and the current price is 14,000 IRR (0.43 USD). In other cities it was 35,000 IRR (11.07 USD), and is now 9,500 IRR (0.29 USD). ([Source](#))

- **March 12:** Deputy ICT Minister Mohammad Javad Azari Jahromi said they are aiming to increase Iran's international bandwidth from 560 Gbps to 30 Tbps by the end of the Sixth Five-Year Plan (2016-2021), but given the lack of private investment in the ICT sector this would prove impossible. Instead, to achieve this goal, he claimed that Iran needed to end the state's monopoly over internet bandwidth by the Telecommunication Infrastructure Company (TIC), and further involve the private sector. ([Source](#))
- **March 12:** ICT Minister Mahmoud Vaezi denied reports suggesting that Telegram would be replaced with an Iranian version of the app, claiming that there were no plans to do so. In other comments he said social media will play a key role during the election campaign, and that such platforms help Iranian citizens to make decisions about how to cast their vote. ([Source](#))
- **March 13:** Seyed Abolhasan Firouzabadi, Secretary of the Supreme Council of Cyberspace (SCC), said Clash of Clans has annual profits of 1.2 trillion IRR (37 million USD) through Iranian users. He also mentioned that the Iranian computer games market is worth 2 trillion IRR (61 millions USD). ([Source](#))
- **March 14:** Mohammad Reza Farnaghi Nezhad, Director of the Public Relations Center of the ICT Ministry said the key achievements for the Ministry were national roaming, Mobile Number Portability (MNP), new licences for 3G and 4G networks, and lastly, increasing the usage of domestic traffic from 10% to 40%. ([Source](#))
- **March 15:** The Russian ICT Minister Nikolay Nikiforov met with Iranian ICT Minister Mahmoud Vaezi in order to bring about further collaboration on ICT-related issues, including internet infrastructure development, software development, e-Commerce and information security. ([Source](#))
- **March 15:** Saeed Reza Ameli, a member of the Supreme Council of Cyberspace (SCC), said 76% of Iranians use circumvention tools. He said this demonstrated the need for citizens to be more educated about cyberspace, and the necessity of producing more religious content. ([Source](#))
- **March 15:** ICT Minister Mahmoud Vaezi said that messages sent by the President's Office will not cost the government, because operators have agreed to charge no fee for it. ([Source](#))
- **March 15:** The Communications Regulatory Authority (CRA) has announced that over 80,000 SIM cards have successfully changed their operator by using Mobile Number Portability (MNP). The CRA said they have received 164,678 requests to use this feature since launching the MNP project. ([Source](#))

- **March 20:** ICT Minister Mahmoud Vaezi announced that his ministry will create 130,000 new jobs in the ICT sector in the new year (March 2017 – March 2018). ([Source](#))
- **March 21:** ICT Minister Mahmoud Vaezi said telecommunications will be improved in preparation for the upcoming presidential and local council elections. He added that the number of internet users has increased from 200,000 to 40 million and he also promised that 90% of villages in Iran will have access to online services by the end of the current government. ([Source](#))
- **March 24:** Secretary of the Strategic Council of National Search Engines said that, in a collaboration with the National Center of Cyberspace (NCC), government organisations were being told to use national search engines in their daily work. ([Source](#))
- **March 25:** Deputy ICT Minister Nasrollah Jahangard said the biggest achievement of the last Iranian year (March 2016 – March 2017) was the launch of two phases of the National Information Network (SHOMA). Jahangard said that by launching SHOMA Iran has developed a secure network that encourages users to use domestic tools. He also mentioned that the third and final phase of SHOMA will launch in May 2017. ([Source](#))
- **March 25:** Seyed Reza Salehi Amiri, Minister of Culture and Islamic Guidance (MCIG), asserted that internet censorship does not help to achieve Iran's cultural objectives, and other approaches should be developed to encourage young people to engage with religious content. ([Source](#))
- **MARCH 25:** The ICT Minister denied reports that the government is negotiating with Telegram and offering to pay the company 800 billion IRR (24.6 million USD) to relocate their servers to Iran. ([Source](#))
- **March 28:** Mahdi Faghihi, the Head of New Technology at the Research Center of Iran's Parliament criticised the ICT Ministry for not providing enough support to domestic industries to create content and software. ([Source](#))

4

Statements from Civil Society and Professional Organisations

- **March 5:** Director of the Computer Trade Organisation (CTO) Naser Ali Saadat said that all businesses and startups seeking to use the internet need to obtain a licence from the CTO. Some startups previously faced closure due to lacking licences, and causing tensions with parallel offline businesses, such as in the case of conflict between taxi-hailing apps [Tap30](#), [Snapp](#) and Tehran's traditional taxi union. ([Source](#))
- **March 12:** Mohammad Ali Yousef Zadeh, Director of the ISP AsiaTech said that the 200 most visited domestic websites are hosted on the National Information Network (SHOMA), and as a consequence users will get 50% off their bill when they visit these websites. ([Source](#))
- **March 15:** Irancell has launched a new service for deaf users that automatically lets callers know that they should message instead. ([Source](#))

5



Surveys and Statistical Data



- **March 4:** The Iranian Students News Agency (ISNA) released statistics on internet users in Iran:
 - ◇ There were 36,856,570 broadband internet users by 22 October 2016, of which:
 - 9,318,943 (25.28%) use ADSL and WiMAX services.
 - 27,170,000 (73.71%) use mobile broadband.
 - ◇ There are 25,269,000 users on 3G and 2,276,000 on 4G. ([Source](#))