Special Report

Filterwatch

Bills, Bills, Bills: Upcoming Policy Challenges in Iran, and How We Can Resist Them

smallmedia.org.uk
Welcome to Filterwatch

Filterwatch is a monthly briefing paper published by Small Media, a London-based not-for-profit organisation working to support freedom of information and freedom of expression in closed societies.

The Filterwatch series (formerly known as the Iranian Internet Infrastructure and Policy report – or IIIP) was first published in 2012 with the aim of documenting documenting the ever-expanding restrictions on freedom of information in Iran, but as the internet policy environment increases in its complexity, so too have our Filterwatch reports expanded to encompass wider issues relating to internet policy and infrastructure development in Iran.

Over the last few years we have documented the development of SHOMA (also known as the National Information Network), adaptations in filtering methods and policies, yearly ICT budget adjustments, and appraisals of Iran’s emerging tech economy. We have also sought to highlight how Iranian citizens use the Internet in their daily life, whether engaging with political campaigns, or connecting with the global community.

Our growing readership is made up of activists, campaigners, policymakers, journalists and academics whose work depends upon up-to-date and reliable information about the development of ICT policy in Iran. We always want to hear from you, and to get your advice on where Filterwatch should go next. We’re often open to partnerships and collaborations, and so if you have ideas around topics to cover, or themes to explore, do get in touch at contact@smallmedia.org.uk.

Thanks!

The Small Media Team
# Table of Contents

**Executive Summary** 3

**Movers and Shakers: Mapping Iran’s ICT Policymakers** 5

- The Majles 7
  - Pervasive Coalition of Reformists / Reform & Moderates 7
  - Principlists Grand Coalition / Conservatives 8
  - The ‘Cyberspace Faction’ / Cross-Party Group 9

- Rouhani Administration 11
  - President Hassan Rouhani 11
  - ICT Minister Mohammad-Javad Azari Jahromi 12

- State Institutions 13
  - Supreme Leader Ali Khamenei 13
  - Judiciary 14
  - Supreme Council of Cyberspace 14

- Other Stakeholders 17
  - Tech Entrepreneurs 17

- The Policy-Making Landscape 18

**On The Horizon: Iran’s Upcoming Legislative Agenda** 19

- e-Governance Bill 20
- Electronic Transactions Bill 22
- Electronic Identification Bill 24
- Intermediary Liability Bill 25
- Data Protection and Online Privacy Bill 27
- Managing Social Messaging Applications Bill 29
- What These Bills Mean 33

**What Comes Next? Potential Threats & Responses** 36

**Credits** 39

**Bills, Bills, Bills – Visualising the Legislative Landscape** 40
Executive Summary

Iran’s ICT policy-making landscape is complex, and for much of the last decade has been in flux. But a new raft of legislation being spearheaded by ICT Minister Mohammad-Javad Azari Jahromi looks set to comprehensively reshape the sphere, potentially ushering in a period of lesser volatility, greater consensus, and likely the continued degradation of Iranian citizens’ digital rights.

For much of President Rouhani’s first term in office, the state’s approach to issues of internet regulation were defined by ongoing conflict between the ICT Ministry and judiciary officials — a battle that spilled over into the Supreme Council of Cyberspace (SCC) and the Committee to Determine Instances of Criminal Content (CDICC) on numerous occasions.¹

But five years into Rouhani’s presidency we believe that Iran’s formerly messy and incoherent processes of internet policy formulation have undergone some significant changes, with ICT Minister Mohammad Javad Azari-Jahromi and his team beginning to articulate a more coherent – and sometimes alarming – vision for the development of the internet in Iran.

In particular, a set of new legislation proposed by Iran’s ICT Ministry – which enjoys the support of the judiciary and the tacit approval of the SCC – looks set to create new legal architectures to govern fields ranging from eGovernment, to data protection, to cryptocurrencies. These new bills will mark the first legislative innovations since the 2010 Computer Crimes Law, and taken together they look set to be even more transformative.

These upcoming bills are:

- Electronic Transactions Bill
- E-Governance Bill
- Intermediary Liability Bill
- Electronic Identification Bill
- Data Protection and Privacy Bill
- Managing Social Messaging Apps Bill

Apart from these bills – of which drafts have been published – we know that other legislation is likely to be brought forward in the next couple of years. These bills will relate to child protection, and cryptocurrency regulation. We also expect significant planning of Iran’s digital sphere to feature in the upcoming Seventh Development plan.

In light of these developments, our team thought it was important to provide an up-to-date guide to the current workings of ICT policy in Iran. In this special edition of Filterwatch, we will provide a comprehensive break-down of how policy is developed, who is engaged in the process, and what is on the current agenda.

We’ll begin by providing a short introduction to some of the leading centres of ICT policy-making power in Iran in the Rouhani era. By moving beyond the traditional dichotomy of ‘reformist’ vs. ‘conservative’, we attempt to explain the multifaceted and complex nature of the policy debates that have been wracking the Iranian ICT policy sphere in recent years.

By mapping these players, we’ll open up new questions about the contestation of policy-making power in the Islamic Republic today, and start to explore how this upcoming legislation sits within this delicate balance of power.

Then, we’ll provide a run-down of the ICT bills that have already been announced by the Iranian government. Based on existing drafts, we will attempt to articulate some of their potential impacts upon citizens’ digital rights – and also to begin to develop a roadmap for pushing back against their most regressive elements.

It should also be noted that this paper will focus only on the upcoming legislative proposals which will require the consent of the Majles, and the Guardian Council before becoming part of Iran’s legislative landscape, and therefore will not be studying the upcoming regulations and resolutions passed by regulatory bodies such as CRA and SCC.

This proposed legislation remain today highly sheltered from much-needed scrutiny. While we acknowledge the importance of non-legislative policies, by providing greater scrutiny to these draft bills we hope to shed light on their importance, and to better understand the processes and stakeholders that will be shaping them.
Movers and Shakers: Mapping Iran’s ICT Policymakers

Over the past decade, Iran’s ICT policy-making landscape has been shaped by a diverse array of stakeholders from across Iran’s political spectrum. Historically, Iran’s policy-making processes have frequently devolved into acrimonious battles between the more authoritarian segments of the state apparatus (typically located in the judiciary) and those elements favouring a more laissez-faire approach to regulation (most notably in Rouhani’s first-term ICT Ministry).

But with the ascendance of Mohammad-Javad Azari Jahromi as Rouhani’s ICT Minister in 2013, the outlines of a more coherent consensus-based policy-making model have emerged.

Jahromi and the New Consensus in ICT Policy-Making

Following his confirmation battle, we argued that Jahromi’s appointment was likely to signal a realignment in ICT policy-making.² We anticipated that his long-standing association with elements of Iran’s security apparatus could lead to a thaw in the relationship between the judiciary and Rouhani’s government.

In reality, this thaw has progressed at a pace beyond our expectations, with policy-making organisations such as the CDICC and SCC enjoying greater prominence and operating on a more consensual basis than they did under the Vaezi Ministry.

It’s unclear whether Jahromi is the architect of this new consensual approach, or merely its executor is unclear, though he does seem entirely comfortable engaging with the judiciary and conservative elements on these policy-making bodies.

With the regularity of SCC meetings stepping up significantly in the last two years (with meetings taking place on a near-monthly basis)³, the publication of a number of flagship policy papers, and plans to bring forward key items of ICT legislation, it seems that the Jahromi Ministry has

---

³ ISNA, ‘Secretary’s comments on filtering, a legislative vacuum and filtering of particular groups’, available at: http://bit.ly/2WEjWKs
made significant progress toward formalising a distributed policy-making process among the main centres of political power in the Islamic Republic.

Through bodies such as CDICC and SCC, the main centres of power in the Islamic Republic—the three branches of government, the security forces, and institutions operating under the Supreme Leader—deliberate policy development and craft a vision for the future of the internet in Iran. Of course, it's crucial to note that the Supreme Leader's representatives have significant influence in all of these institutions and processes shaping internet governance in Iran.

In this sense, Iran has designed its own version of multistakeholder internet governance—one that lacks representation from civil society, internet users, and businesses—but which formalises a policymaking procedure among the political elite which facilitates structured debate and consensus-building on key questions of policy and infrastructure development in Iran.

So before we go any further, let's meet the key players in this new policy-making landscape, in order to better understand their interests and policy priorities moving forward.
The Majles

First off, let’s give some attention to Iran’s parliament – the Majles.

Up until recently, Iran’s Majles has tended to take a backseat in the development of ICT policy. Iran has only passed one major piece of legislation governing the internet and users’ digital rights. The restrictive 2010 Computer Crimes Law was passed in the aftermath of the disputed 2009 presidential elections, and since then has frequently been deployed in support of the state’s systematic crackdown on online expression.

Now, Rouhani’s administration (or more accurately, Jahromi’s ICT Ministry) is working to introduce a raft of far-ranging ICT legislation to formalise internet regulations and to more clearly delineate Internet users’ rights – legislation that will need to be reviewed and approved by the Majles before entering into law.

Over the past five years, the ICT Ministry has yet to face any significant pushback from Parliament on its agenda, perhaps coming closest to a defeat in the case of Jahromi’s confirmation vote. Jahromi only just scraped through his hearing after the Reformist faction (headed by former presidential candidate Mohammad Reza Aref) mobilised in support of his nomination.

But is there any prospect of this new slate of bills facing similar levels of opposition? There are three overlapping coalitions of MPs that the ICT Ministry will need to appease if the bills are to pass through the Majles smoothly.

Pervasive Coalition of Reformists / Reform & Moderates

The Pervasive Coalition of Reformists (PCR) grouping of reformists and moderates in Parliament, elected in 2016 under the List-e Omid (or ‘List of Hope’) are the key allies of President Rouhani in the legislature. Although elected under a single list, the grouping is not tightly bound by any party structures or disciplinary procedures, and individual members’ voting record is not subject to public scrutiny.

The group’s central pledge at the parliamentary election was to support Rouhani’s government, and so it follows that any ICT-related legislation
put before the grouping by Jahromi’s ICT Ministry is likely to enjoy a healthy level of support.

However, many MPs from the grouping identify themselves in the reformist political tradition, and have an obligation to closely scrutinise any new bills that are put before the parliament, and ensure that they do not adversely impact upon the rights of Iranian citizens to freedom of expression and privacy.

It is this sub-grouping within the PCR that should be pressured most intensively to scrutinise and resist any new legislation that might threaten Iranian citizens’ digital rights.

Principlists Grand Coalition / Conservatives

The leading conservative coalition the Principleists Grand Coalition (PGC) performed relatively poorly in the 2016 legislative elections, securing only 83 of the Majles’ 290 seats. Regardless, conservatives in the Majles still enjoy a significant degree of influence over the passage of bills in the legislature.

Despite the PCR’s numerical advantage, conservatives have been able to retain a tight grip on a number of parliamentary committees, which could see them representing these committees on any new regulatory bodies formed in the coming months. In this sense, conservatives could end up wielding significant influence over policy development and implementation regardless of their poor electoral showing.
The ‘Cyberspace Faction’ / Cross-Party Group

On 24 October 2018, Ehsan Ghazizadeh-Hashemi—the MP for Fariman and a former official of the Ahmadinejad-era Ministry of Culture and Islamic Guidance—announced the formation of a new “Cyberspace Faction” in the Iranian Parliament. The group claimed the support of 71 members from across a number of parliamentary groupings. Ghazizadeh, who is a member of the Committee on Cultural Affairs, discussed the need for further ICT legislation in his announcement.

Three other leading members of this group – Jabbar Kouchakinejad, Ahmad Amirabadi and Sadegh Tabatabainejad – are significant in that all are members of parliamentary committees, suggesting that the emerging ‘faction’ is seeking to mobilise members across a number of influential committees such as the Culture Committee and Industrial Committee, where they could influence the passage of bills as they undergo parliamentary review.

Members of this faction put forward the controversial “Managing Social Messaging Apps Bill” in late 2018, which threatens to hand over control of significant segments of Iran’s internet infrastructure to the armed forces.4

While it comes as little surprise to find the name of senior MPs from the new ‘Cyberspace Faction’ among the supporters of the bill, it is deeply troubling to see the name of 25 reformist MPs among the supporters of the first draft. These names included high-profile reformist MPs such as Alireza Mahjoub. The fact that this proposed bill enjoys a level of support among reformist MPs raises questions about the ability and willingness of reformist officials and representatives to stand up for citizens’ rights online.

---

Moving forward, pressure should be imposed upon reformist MPs to reject the agenda of this emerging faction, which so far appears to favour a policy agenda that runs counter to the advancement of citizens’ rights.

Discontent and pushback against the Managing Social Messaging Apps Bill amongst reformist MPs has already taken place,5 casting some doubt over the proposed legislation’s future, and over pro-reform MPs’ place in this ‘Cyberspace Faction’ in the months ahead. Such pressure should therefore be sustained.

Rouhani Administration

The Rouhani administration, after spending much of its first term prioritising ICT infrastructure investment and resisting the judiciary’s attempts to filter online platforms and content, has in its second term started to take a more proactive role in devising and proposing new regulatory frameworks to govern the Internet’s further development.

A lot of this work has been spearheaded by ICT Minister Mohammad-Javad Azari Jahromi, who has taken an undeniably more energetic approach to the job than his predecessor Mahmoud Vaezi. President Rouhani and Jahromi together exert a great deal of influence over the development and implementation of new legislation.

Despite using the issue of digital rights as a wedge issue during both of his election campaigns,⁶ Rouhani and his administration have failed to legislate in any way that improves digital rights in Iran. Although the administration launched the ‘Charter on Citizens’ Rights’ and the five bills here outlined here, none have so far been submitted to the Majles for formal consideration.

Although the Rouhani administration has spent the last two years developing policy consensus around these slated bills, it is rapidly approaching the point where it will need to secure legislative approval.

President Hassan Rouhani

In 2013, Rouhani brought a degree of hope to Iranian internet freedom activists. He explicitly promised the liberalisation of cyberspace in Iran, and his government’s commitment to SHOMA was initially viewed as lip service to appease conservative critics. His government invested in national internet infrastructure to expand access, improve speeds and reduce the cost of connectivity for average users. Hope was also fostered by then-ICT Minister Mahmoud Vaezi’s timely public debates with conservatives and judiciary representatives on the CDICC, which suggested to some that Rouhani aimed to curtail Iran’s use of internet controls.

President Rouhani maintains an outspoken public stance on the issue. In a televised address in January 2019 he criticised the practice of internet censorship in Iran, stating that perceived challenges posed by an open internet were rooted in Iran’s closed media environment: “We do not have media freedom in Iran. We have only a state-owned radio-television. So, everyone has rushed to social media... People want to say everything on social media because we do not have any other media outlets.”

Although President Rouhani presents himself as a staunch opponent of censorship, he ultimately retains a great deal of influence over the future direction of ICT policy — he chairs meetings of the SCC, and his cabinet ministers take up a large proportion of seats on the CDICC.

His appointment of Jahromi as ICT Minister also points towards a more complicated picture of Rouhani’s record than his public statements may offer – although a stated opponent of filtering, Jahromi’s profile is not that of a typical reformist, and his vision for the Internet in Iran is far from a liberal one.

ICT Minister Mohammad-Javad Azari Jahromi

Much is made of ICT Minister Jahromi’s young age – at On 20 August 2017 the Iranian parliament voted to approve President Rouhani’s nominee for the position of ICT Minister. Mohammad-Javad Azari Jahromi, former Deputy ICT Minister and CEO of the Telecommunication Infrastructure Company, was confirmed by 152 votes to 120.

His narrow victory came against the backdrop of a chaotic confirmation hearing in which he faced accusations of complicity (and even active involvement) in the crackdown on protesters after the widely-disputed 2009 presidential election in his former role at the Intelligence Ministry.

Reformists, activists and even some conservatives were quick to attack Jahromi’s record, and his ability to run for office. In an effort to gain support for Jahromi, Rouhani emphasised Jahromi’s youth, highlighting the fact that he is the first serving cabinet minister to have been born after the 1979 Revolution. Jahromi also boasted about his support within the burgeoning tech industry. Although these words may have given

---

Jahromi the edge he needed, his confirmation was far from an easy ride. His history hung heavily over him.

State Institutions

In addition to the elected Rouhani government, a number of unelected state institutions and individuals exert significant influence over the development of ICT policy in Iran. The most significant of these actors is the Supreme Leader Ali Khamenei, who in turn exerts a great deal of influence over the Iranian judiciary, and Iran’s highest ICT policy-making body, the Supreme Council of Cyberspace.

Supreme Leader Ali Khamenei

Iran’s Supreme Leader is without a doubt the most powerful political figure in Iran, but by no means does he hold all the power. On the question of Internet governance and digital rights, Khamenei has demonstrated time after time that he favours the imposition of strict controls on the Internet. With the establishment of the SCC, Khamenei has sought to centralise policy-making in Iran, and to heavily influence its development through his political appointees to the body.

On 5 September 2015, Khamenei appointed new SCC members for four-year terms, and outlined their tasks in ten points. Apart from urging further progress on SHOMA, Khamenei also made it clear that he wanted the SCC to bring forward new policies and regulations.

Since then, Khamenei has remained largely disengaged from debates around regulation and details of policy development. Without commenting on specific issues, he has issued a number of complaints about slow progress in the development and implementation of SHOMA.

His most significant intervention, however, was a recent fatwa declaring that invading the privacy of internet users is forbidden. This was a significant move, coming about owing to continued public mistrust in domestic messaging apps.6 His fatwa can be taken as a clear indication of

---

his desire for the government to work harder to gain public trust on data protection, and to roll out new legislation to that effect.

The proposed Data Protection and Privacy Bill appears to have been developed with this imperative in mind, though its contents do little to inspire confidence – it contains myriad loopholes that threaten to undermine citizens’ digital rights in the long-term.

Judiciary

The Iranian judiciary is under the direct influence of the Supreme Leader, through the appointment of all of its senior officials. The current Judicial Deputy on Cyberspace Issues, and Secretary of the CDICC Javad Javidniya – like his predecessor Abdolsamad Khorramabadi – has been a vocal advocate for a stricter filtering regime.9

The judiciary has often used its powers to bypass the CDICC in filtering websites and apps (such as in the case of Telegram).10 However in recent months, the judiciary appears to have found common cause with the ICT Ministry on the issue of determining the new ICT-related legislative frameworks required in Iran, taking a leading role in drafting new legislation.

Supreme Council of Cyberspace

In March 2012, Supreme Leader Khamenei issued a decree that authorized the establishment of the Supreme Council of Cyberspace (SCC) as the focal point for national ICT policy-making and coordination.

The decree demanded that all other organisations and institutions cooperate fully with the SCC’s rulings. Similar to other Supreme Councils, the SCC is comprised of 17 institutional members and eight of the Supreme Leader’s political appointees. In September 2015 Khamenei

---

renewed the mandate of the SCC with the following institutional appointees:11

- President (Chairman of SCC),
- Parliamentary Speaker
- Chief Justice
- ICT Minister
- Attorney-General
- Education Minister
- Defence Minister
- Intelligence Minister
- Culture and Islamic Guidance Minister
- Science Minister
- Head of the National Center for CyberSpace
- Head of IRIB
- Head of the Islamic Development Organization
- Head of the Parliamentary Cultural Committee of Majles
- Vice-President for Scientific and Technological Affairs
- National Police Chief
- Chief Commander of IRGC

In the same decree the following individuals were also added as political appointees:

- Seyyed Saeed Reza Ameli,
- Hamid Shahryari,
- Reza Taqipour,
- Mehdi Akhavan Behabadi,
- Masoud Abou-Talebi,
- Kamyr Saqafi,
- Rasoul Jallili
- Ezzatollah Zarghami

The Supreme Leader exerts extensive authority over SCC in three ways:

1. Make political appointments to the SCC
2. Approve the SCC’s election of the body’s Secretary
3. Approves the resolutions passed by the SCC.

SCC decisions are enforceable as law even though there is no particular law or supervising institution that expressly oversees the Council. SCC resolutions are directly sent to the Supreme Leader for approval with no oversight from either the Majles or the Guardian Council. Additionally, the Leader’s official endorsement of SCC resolutions extends more legitimacy to them than to laws passed by the Majles.

SCC resolutions that are not approved by the Leader are considered to be lower in status than other laws, although this is a moot point – all SCC resolutions thus far have been endorsed by the Supreme Leader.

These circumstances enhance the possibility of legal discrepancies. To avoid such legal confusion, several legal scholars have entertained the idea of a bill that outlines the scope of authority of SCC to be considered by the parliament. Alternatively, they recommend deferring SCC resolutions to the parliament or Guardian Council to review for consistency with higher laws.\(^\text{12}\)

Among the resolutions that SCC has passed in recent years, two are more consequential than others. The first is the March 2015 resolution on ‘Development of Healthy, Positive, and Safe Cyberspace’\(^\text{13}\) and the second is the April 2016 ‘Decision Regarding Parallel Supreme Councils’.\(^\text{14}\)

The resolution on the **Development of Healthy, Positive, and Safe Cyberspace** defines “healthy, positive, and safe cyberspace” as a virtual space containing communication networks that provides “useful” content and services in accordance with Islamic principles and values and national laws. It states that users can benefit from such a healthy virtual environment based on their demographic needs (for example, age, gender, education, and occupation). To the extent possible, they should also remain safe from exposure to “harmful” online content and behavior.

This resolution clearly laid out the policy priorities for Iran’s ICT policy-making institutions in Iran, and gave direction to the SCC’s future work. Since 2015, the body has taken a far more active role in domestic content production and promotion, with a particular view to strengthening and promoting SHOMA. As part of this approach, the SCC has also embraced domestic software development and promotion with the ultimate goal of replacing popular social media platforms such as Telegram and Instagram and blocking access to foreign services.

The **Decision Regarding Parallel Supreme Councils** was also significant in that it dissolved four other Supreme Councils (three of which were responsible to the President) and folded their powers into the SCC. This move strengthened the influence of the Supreme Leader in policy discussions – although the SCC is chaired by President and includes a fair number of cabinet ministers, the number of Supreme Leader appointees is significant enough to exert influence on many debates.


Its broad powers, and the incorporation of perspectives from the Rouhani administration and the Supreme Leader’s chosen experts means that the SCC retains its paramount position in the ICT policy-making landscape, and looks set to retain this in the years ahead as future legislation is debated and eventually implemented.

Other Stakeholders

Non-state-affiliated stakeholders have typically been shut out of major ICT policy-making decisions in Iran, with consultative multi-stakeholder processes far from the norm. However, proposed legislation hints that there may be some scope for segments of the Iranian private sector to be brought into emerging discussions in a number of fields – but most worryingly to potentially participate in the state’s information controls agenda.

Tech Entrepreneurs

Iran’s policies of cultural and economic protectionism – as well as the conditions imposed by international sanctions – have meant that the Iranian market has been largely inaccessible to global tech companies. This has led to the growth of a significant domestic community of tech entrepreneurs, who have been able to take advantage of this vacuum.

Iran’s tech entrepreneurs should be divided into two broad groups: those whose business is dependent on the filtering of foreign websites and apps, and those who are not (and whose operations have frequently been hampered by the filtering regime in Iran).

ICT Minister Jahromi has been very keen to develop a good relationship with Iran’s community of tech entrepreneurs, and upon his confirmation he was mostly received as a friend of small businesses and tech startups. However, the at-first temporary, and then permanent ban of Telegram following the protests in January 2018 severely bruised his relationship with a number of tech entrepreneurs.

Although the filtering regime negatively affects many tech entrepreneurs, those who currently benefit from filtering and ongoing government support for domestic messaging apps have been vocal in their demands for further legislation.
The Policy-Making Landscape

So far during Rouhani’s second term, policy-making bodies have largely adapted to their new roles in the new consensus-based regime. Although the judiciary has continued to act unilaterally at times – including in its imposition of filtering on Telegram – Iran’s broader policy decisions relating to the Internet are governed in accordance with the balance of power across key institutions like the SCC and Majles.

The continued centrality of the SCC in high-level policy development has so far delivered growing consensus between Rouhani and political appointees of the Supreme Leader who sit on the council, with this consensus going on to inform the policy initiatives of the ICT Ministry.

However, if the named pieces of legislation – and possibly others – make their way into the Majles to seek parliamentary approval, this consensus could be tested. Once in the legislature, conservatives and pro-reform MPs may end up taking positions less in line with the consensus established on the SCC.

In this sense parliamentarians may be able to leverage their own influence over the process to rechart the course of this legislation, and bring its provisions more into line with their own priorities for national ICT policy. It is important therefore that civil society can provide MPs with the information and tools they need to make informed decisions about how to progress ICT-related legislation in the coming months and years.
On The Horizon: Iran’s Upcoming Legislative Agenda

In March 2018 a conference of Iran's Judiciary Research Institute published five draft ICT regulation bills for consultation. Later, in July 2018 the Data Protection and Privacy Bill was submitted to the cabinet for consideration. The other four bills have not yet been moved forward, but all will ultimately need to secure parliamentary approval to enter into law. The proposed legislation addresses a large number of gaps in existing ICT law, and have potentially significant implications for the current structure of electronic governance, entrepreneurship and commerce.

The bills introduce new regulations on online privacy, e-governance, electronic identification and transactions, as well as intermediary and service provider liability.

In addition, the newly-formed ‘Cyberspace Faction’ in Iran’s Majles has drafted its own bill to regulate and encourage the development of domestic messaging apps. This legislation has been criticised by a number of centres of power in the state apparatus, but may yet find a path through the legislature.

In this segment of our report, we’ll run through each of the proposed new bills in turn, and explain the potential ramifications of this new raft of legislation on the digital rights of Iranian citizens.
# e-Governance Bill

The e-Governance Bill\(^\text{15}\) introduces regulations that apply to all state agencies and entities, including legislative, executive, and judicial bodies, the Office of the Supreme Leader and all its subsequent entities, public non-governmental bodies, and institutions in charge of public assets and services.

<table>
<thead>
<tr>
<th>Objectives</th>
<th>The bill sets out rules for electronic mechanisms that these bodies have already established – or will embrace in the near future – in order to interact with one another, provide public services, and perform other responsibilities.(^\text{16}) These rules apply to national and transnational aspects of e-governance (Article 19).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The bill pursues multiple objectives such as improving the performance of state bodies, enhancing the transparency of official procedures, and improving the public’s access to information and participation in public decision making processes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transparency</th>
<th>To ensure transparency in governance, the bill requires all relevant state bodies to ensure to publicise all information regarding:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>(a)</strong> rights and responsibilities regarding e-governance procedures and the implementers;</td>
</tr>
<tr>
<td></td>
<td><strong>(b)</strong> any supporting information/content such as surveys and survey results, and;</td>
</tr>
<tr>
<td></td>
<td><strong>(c)</strong> any information about exchanges among decision makers and regulators and their statements that pertain to this bill, and their legal implications for end beneficiaries (Article 41).</td>
</tr>
<tr>
<td></td>
<td>However, a few types of public electronic announcements are exempt from such exercise of transparency. These exceptions apply to confidential information, personal and private data, and any other information that their publication needs judicial or law enforcement order or approval (Article 66).</td>
</tr>
</tbody>
</table>

| Disability Rights and Accessibility | In a progressive move, the bill acknowledges disability rights by stipulating that any public notifications become accessible to audiences with disabilities (Article 54). |

\(^{15}\) The full text of the e-Governance Bill is available at: [http://bit.ly/2v5mFZ](http://bit.ly/2v5mFZ)

\(^{16}\) For example, ‘Electronic Executive Affairs’, which include any procedures and information pertaining to legal protections for identities, events, measures, etc. (Articles 7-9), ‘Electronic Judicial Affairs’ encompasses all procedures and information that deal with criminal, civil, and governmental lawsuits and regulatory, law enforcement, and sectoral misdemeanors (Articles 13-15).
Restrictions on Data Hosting
The bill endorses the use of national information network (NIN) and prohibits hosting of any e-governance data outside of Iran (Article 76). In addition, the use of cloud services for matters of e-governance is contingent upon taking “the interests of all stakeholders” into consideration, although at present these stakeholders remain undefined (Article 78).

Electronic IDs
The bill defines electronic IDs in the same way as the Electronic Identification Bill, and provides examples of each ID type for humans, living creatures (including plants and animals), tangible and intangible goods, geolocations, and cyber identifiers (Article 81).

Bill Implementation
To ensure comprehensive implementation of the bill, a leadership mechanism is defined which comprises of a Supreme Commission, seven specialized (expert) commissions, and their secretariats.

The Supreme Commission will be composed of:

- Vice President
- Vice Head of the Judiciary
- Head of National Center for Cyberspace (NCC)
- Chief of Staff of Armed Forces
- An expert appointed by the Head of the Parliament
- ICT Minister (serves as the Commission’s secretary)

Expert commissions will focus on matters of their specialty:

1. **Defense and Law Enforcement** – in charge of cyber defense, including preventive, passive, and active defense among other responsibilities;
2. **Political and Security Affairs** – in charge of electronic elections and preventing political and security-related crimes;
3. **Culture and Media** – in charge of soft war defense;
4. **Commerce and Trade** – regulating virtual markets;
5. **Education, Research and Technology** – in charge of e-education;
7. **Legal and Judicial Affairs** – in charge of electronic procedures within the justice system.

The bill evidently envisions that new areas of governance may arise as the application of ICTs introduces transformative impacts on society over time. As such, each commission is responsible for addressing a set of issues within their scope of work. Examples include determining procedures of e-governance within their scope of work, identifying needs within their fields of expertise, and estimating costs for providing e-governance services, addressing complaints, and coordination with other commissions (Article 138).
**Electronic Transactions Bill**

This bill\(^\text{17}\) seeks to develop a coherent system to regulate electronic transactions. It accredits e-transactions (e.g. commercial and personal transactions) as legal instruments, and validates electronic services offered by state offices.

By endorsing and enhancing the scope of e-transactions, the bill also promotes e-government services, and supports new uses of ICTs in commerce and other areas. Most importantly, it affects regulations on e-signatures that Iran’s e-commerce law had previously established. This bill replaces e-signatures with trusted and credible e-IDs that will be used to validate e-transactions.

| **Defining e-Transactions** | The bill defines ‘e-transactions’ as “any automated or semi-automated procedures through electronic portals that process and document computer data”. According to the bill, ‘data processing’ is defined as “any intentional creation, changing, sending, receiving, transporting, removal, sharing, or displaying of data”. The regulations therein apply to three categories of electronic transactions:  
1. Public transactions that are processed by any state entity that the bill addresses.  
2. Private transactions that are processed by private institutions.  
3. Personal transactions that occur among private individuals. |
|---|---|
| **Transaction Data** | The bill entitles anyone to search and access any of their transactions’ data. Such data can be used as a legal instrument in court (Article 7). However, in a progressive move, the bill does not recognize transactions’ data that are obtained illegally and negates their credibility in court (Article 8). Interested parties or their legal representatives can request access to transactions data, either in writing or electronically (Article 9).\(^\text{18}\)  
In the case of a lawsuit or criminal proceedings, providers of digital access (e.g. mobile networks, VoIP, and WiMAX), hosting, software, and other ICT services are all required to cooperate and prepare electronic transactions data such that they can be used as legal instruments. |


\(^{18}\) In a logical loop, the bill states that data processors are not allowed to process e-transactions data “without the knowledge of interested parties” unless the law requires so, or with “express consent of data owners”. It is unclear how someone may expressly consent to processing their data without having knowledge about the matter.
| **e-Transactions and e-IDs** | E-transactions are verified based on data from electronic IDs that are described in the electronic identification bill *(Article 36)*. Electronic IDs can be revoked by the following authorities or circumstances:
- Court or prosecutor order
- Death of individual, dissolution of incorporated institutions, or if data servers become permanently unavailable.
- Expiration of e-IDs
- At the request of e-ID holder. |
| **e-Transactions and Criminal Acts** | The bill also penalizes several acts in accordance with the 2010 Computer Crimes Law e.g. illegal wiretapping, interception, inspection and withholding of data.

To determine criminal acts that may have occurred within the jurisdiction of Iran, the bill considers any e-transaction through country code top-level domains (ccTLDs) such as .ir, .iran.ir, iran.ac.ir or their Persian equivalents (for example: ایران) within the Iranian jurisdiction. The perpetrator of a criminal e-transaction can be prosecuted in Iran only if (s)he is in the country, or can be extradited to the country. |
## Electronic Identification Bill

The Electronic Identification Bill\(^{19}\) seeks to enhance coordination among relevant authorities who regulate and verify electronic IDs. To ensure compatibility with international standards, the bill provides technical and administrative prerequisites for e-identification.

<table>
<thead>
<tr>
<th>Types of Electronic Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>The new regulations apply to all matters that a virtual ID can be assigned to, including human beings, animals, plants, goods, physical and intellectual assets, geographical locations, and cyber domains. In particular, they include:</td>
</tr>
<tr>
<td>- <strong>Human IDs</strong> such as digital signature, international mobile subscriber identity (IMSI)(^{20}), encryption keys, passwords, etc.</td>
</tr>
<tr>
<td>- <strong>IDs for living creatures and goods</strong> such as biometrics, Digital Object Identifier (DOI), Interactive Object Definition (IOD), International Standard Serial Number (ISSN), barcodes, radio-frequency identification (RFID), and stocks.</td>
</tr>
<tr>
<td>- <strong>Geolocation IDs</strong> such as postal/ZIP codes, Global Positioning System (GPS), Geocodes, landlines and fax numbers.</td>
</tr>
<tr>
<td>- <strong>Cyber IDs</strong> such as ccTLD and generic top-level domains (gTLD), Universal Resource Identifier (URI) and Universal Resource Locator (URL), Persistent Uniform Resource Locator (PURL), and Unique Reference Number (URN).</td>
</tr>
</tbody>
</table>

By observing these extensive categories of identification, the bill paves the way towards regulating new aspects of ICTs such as online entrepreneurship, Internet of Things (IoT), and domain administration that were not previously addressed in Iran’s legal system. In a nod to the right to privacy, the bill also considers any information about electronic IDs of users as private data that cannot be commercialized or exploited.

<table>
<thead>
<tr>
<th>Validation and Controls on Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>The bill requires legally incorporated providers of electronic identification services to acquire due certificates from Ministry of ICT. They will then be the official validators of e-transactions. In an effort to avoid the monopoly and interference of government with matters of e-identification, the bill prohibits executive bodies to offer such services unless (1) electronic IDs are used for public information, (2) private sector does not have enough incentive to enter the market, or (3) it is not economically viable to outsource the identification process to other sectors, or it is exclusive to the government by nature.</td>
</tr>
</tbody>
</table>

---


\(^{20}\) IMSI is a unique number, usually fifteen digits, associated with Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users. The IMSI is a unique number identifying a GSM subscriber. (It is unprecedented that a SIM card number can be used as an identifier for humans)
# Intermediary Liability Bill

The Intermediary Liability Bill\(^{21}\) is based on five principles: free and unlimited access to “legal” information, protection of social, cultural, intellectual rights of all individuals, respect to freedom of speech and opinion, protecting security and privacy, promoting ICTs in the society.

The proposed document seeks to regulate both sides of digital information sharing services: (a) service providers and (b) subscribers and users. The former include providers of access, hosting and data servers, and domain registration services. Providers of access services include international internet exchange points (IXPs), Internet Service Providers (ISPs), and coffee nets.

## Service Provider Responsibilities

The bill defines the rights of users and subscribers in relation to service providers. The latter is responsible for informing the former of all technical opportunities and services that they make available based on pre-established rates and fees.

In addition, service providers are responsible for making due efforts to keep their subscribers and users informed of the rights and responsibilities that this bill would establish for any interested party. Providers are also required to protect all rights, including intellectual rights, of data that users and subscribers place on their network for information sharing purposes.

## User Responsibilities

On the subscribers and users side, the bill requires them to act within the scope of their contracts and legal rights to ensure seamless services are provided by intermediaries. Otherwise, they can be penalized in accordance with the Computer Crimes Law.\(^{22}\)

## Defining ‘Illegal’ Information

The bill defines the following information as “illegal”:

- Insult to religions and holy books, major prophets, Shi’ite Imams, and the daughter of prophet Muhammad;
- Insult to the founder of the revolution i.e. Ayatollah Khomeini or the Supreme Leader;
- Information publishing which is considered as crimes against national security; and
- Disseminating lies or fabricated facts (see more under Article 5).

---


\(^{22}\) Individuals found guilty of “interfering with computer systems” can face a sentence of up to two years in prison and/or fines (Article 8 of Computer Crimes Law).
| Internet Exchange Point Liability | IXPs are responsible to take any necessary measures and utilize the latest technology to ensure that no illegal information is transmitted through their networks. If IXPs fail to do so and ISPs and coffee nets knowingly facilitate the transmission of illegal data, they will be held responsible (**Article 6**). |
| Encryption Requirements | To increase the security and privacy of personal communications, this bill requires service providers to offer appropriate encryption services to users and subscribers (**Article 9**). |
| Personal Communications and Judicial Compliance | The bill prohibits providers of access services from interfering with or changing personal communications data (for example by retrieving or changing passwords) or taking any action that may lead to such results (**Article 10**). However, they are required to cooperate with law enforcement or representatives of the justice system in accordance with current law and regulations (**Article 14**). |
Data Protection and Online Privacy Bill

This bill defines personal data and the parties concerned and elaborates on their rights and responsibilities. It authorizes owners of personal data to directly access or control access to their data at will and within the scope of new regulations. The bill has clearly aspired to GDPR for defining the core legal concepts and procedures. In many instances, the definitions provided therein are close to, or even identical to GDPR. The bill refers to Chapter 3 of the Constitution on the nation's rights and other legal and normative precedences to establish new regulations on data privacy.

<table>
<thead>
<tr>
<th>Definition of ‘Sensitive Data’</th>
<th>The bill defines sensitive data as “any piece of information that reveals tribal and ethnic roots, political, religious, and philosophical opinions, genetic features, or medical information about a person”. Notably, there is no mention of financial information in this definition.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory Jurisdiction</td>
<td>New regulations proposed therein apply to (1) all Iranian citizens and public and private institutions that have been incorporated in Iran, regardless of where their private data is processed, and (2) foreign individuals or public and private corporations whose data is processed by an Iranian controller or processor (Article 3).</td>
</tr>
<tr>
<td>Data Processing</td>
<td>Articles 4-7 stipulates regarding processing of public and non-public data. Express consent of data owner is required for processing their non-public data (Article 4). Consent has to be expressly given prior to processing and needs to indicate understanding of what their consent covers (Article 5). Expressing consent afterward does not legitimize any prior acts. In addition, if individuals have personally published any data (e.g. public Twitter profile pictures) without restricting or blocking access to it, such data are considered as publicly available (Article 6). Processing public data without consent of their subjects is permitted, under the bill.</td>
</tr>
<tr>
<td>Right to Be Forgotten</td>
<td>The bill notably recognizes the right to be forgotten for individuals who are the subjects of the data in question (Article 9). They can request their data to be (or not be) processed if (1) data or the processed outputs are incorrect, and (2) collected or processed data are outside of the scope of their consent. (Article 8). Lastly, if someone consents to processing their data, this consent should not be taken as consent to a breach of their anonymity online (Article 11).</td>
</tr>
</tbody>
</table>

24 Specifically, it refers to Articles 19, 20, 22, 23, 25, 26, 38, and 39.
25 Other normative precedences include the Supreme Leader's April 2018 fatwa on a religious ban on the violation of privacy.
Data Retention and Transit

In case of a personal data removal, controllers and processors must keep data and log files for six months. This can be extended up to 2 years at the request of the oversight commission (Article 33).

Processing of data that belong to Iranian citizens or institutions must be done at domestic data centers or foreign centers that are approved by Iranian authorities. Data transit must be done through secure communication networks (Article 38) but the bill provides no definition for secure in this context.

Implementation Bodies

To promote coordination on privacy-related matters, the bill constitutes four new bodies for the implementation of these new regulations. These include Commission of Personal Data Protection and its secretariat, Oversight Committee (Committee), and specialized working groups (WG). Head of National Cyberspace Center (NCC) sits on both Commission and Oversight Committee.

The Commission's members are:

- Minister of ICT (Commission Lead)
- Minister of Intelligence
- Minister of Internal Affairs
- Minister of Justice
- Minister of Culture and Islamic Guidance
- Minister of Economy
- Secretary of SCC and Head of NCC
- Deputy Head of the Judiciary for prevention of crimes
- Head of the Article 90 Parliamentary Commission
- Attorney General
- Secretary of the Executive Council of ICT who also serves as the secretary of the Commission

The Commission is in charge of coordinating with the Committee and WGs. It can change or modify the responsibilities and members of the WGs. The Commission also resolves disputes among the WGs, the Committee, and other state entities. It would report to higher ranking bodies on data protection measures and standards and would propose practical resolutions and legal measures to said authorities.

The Oversight Committee sits at the Ministry of Justice. Its members are:

- Minister of Justice (who leads the Committee)
- Head of the Article 90 Parliamentary Commission
- Head of NCC
- Secretary of the Commission.

The Committee oversees all oversight-related aspects of the work by the specialised working groups.
## Managing Social Messaging Applications Bill

This bill\(^{26}\) is the only of the slated bills not to have been devised and developed by the ICT Ministry and judiciary. Instead, it was drafted by members of the Majles ‘Cyberspace Faction’ – an informal coalition of MPs who have stated their commitment to legislating on new Internet regulations.

The bill is designed to address the legal gap in the increasingly growing use of foreign social messaging applications by Iranians. It also seeks to promote domestically developed messaging applications at the cost of violating net neutrality and giving clear preference to their traffic. By outlining these legal parameters, the bill paves the way for the state’s access to traffic or data stored on social media applications.

<table>
<thead>
<tr>
<th>Defining Social Messaging Apps</th>
<th>The bill broadly defines social messaging application as “User-based systems that provide platforms for interactions and the collection, broadcast and publication of social information for the purpose of establishing personal or group communications and providing online services such as financial payments and multimedia content” (Article 1). Such definition of a social messaging apps might include news and other websites that permit visitors to post comments.(^{27}) Data protection is defined as “preserving users data” and “preventing any unauthorized access to, exploitation or exposure of such data” (Article 1).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulation and Operational Licenses</td>
<td>According to the bill, the release of all domestic and non-domestic messengers to the Iranian market and their operations are contingent upon their registration in Iran and compliance with national laws. These apps are required to operate under the supervision of an oversight committee that would be vested with the powers of both granting operational licenses, as well as banning them. The ICT Ministry would be responsible for blocking access to any applications that operate without due authorisation.</td>
</tr>
<tr>
<td>Oversight Committee</td>
<td>“Influential” apps are only allowed to operate with permission from the Oversight Committee, which is also responsible for determining the criteria for “influence”. In doing so, the Committee considers factors such as the number of registered users, monthly, weekly, and daily</td>
</tr>
</tbody>
</table>

---

\(^{26}\) The full text of the Managing Social Messaging Applications Bill is available at: [http://bit.ly/2HSBm2X](http://bit.ly/2HSBm2X)

active users, growth rate of an app’s user base, the type of service it provides, and the amount of traffic it carries (**Article 6**).

The committee acts in accordance with the resolutions passed by the Supreme Council of Cyberspace (SCC). Its decisions are final but concerned parties can pursue legal action in the court.

The committee would comprise of various governmental and military agencies as well as individual advisors, including:

- Chairman of the National Cyberspace Center (Committee Chair),
- Deputy Communications Minister or authorised representative,
- Deputy Islamic Guidance Minister or authorised representative,
- Deputy Intelligence Minister or authorised representative,
- Deputy Prosecutor General or authorised representative,
- A member of the Parliamentary Committee on Cultural Affairs,
- Islamic Republic of Iran Broadcasting (IRIB) representative,
- Islamic Revolutionary Guard Corps (IRGC) representative,
- Islamic Propagation Organization representative,
- Police representative,
- Passive Defense Organization (PDO) representative,
- Domestic messengers app representative,
- Shia seminary schools representative.

Most of these representatives are already members of the Supreme Council of Cyberspace (SCC) and the Committee for Determining Instances of Criminal Content (CDICC), and are in charge of similar duties.

However, the bill provides little detail as how the Oversight Committee will be coordinating and interacting with the SCC and CDICC, the highest authorities in Internet policy making bodies. It simply mentions that the Committee's secretariat will be sitting at the NCC.

It is also notable that the bill gives clear operational advantages to domestic platforms, by providing a seat for them at the decision-making table.

<table>
<thead>
<tr>
<th>Compliance – Domestic and Foreign Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>All domestic and foreign apps need to comply with the new regulations within two months of ratifying of the bill into law. However, foreign apps can only be authorized to operate after the completion and launch of national information network and approval of SCC regarding NIN’s completion (<strong>Article 10</strong>). This provision can prolong and complicate the approval process for foreign apps and clearly favors domestic apps instead.</td>
</tr>
</tbody>
</table>
| Transfer of Powers to the Armed Forces | In order to secure data privacy, Article 12 deems armed forces as the ultimate authority in charge of “protecting digital borders and cyber defense to prevent exploitation of data at exchange points of national bandwidth”. The extent and limits of responsibilities will be proposed by the General Staff of the Armed Forces (GSAF) and approved by the Commander in Chief of the Armed Forces i.e. the Supreme Leader. We would also not that “digital borders” is an abstract concept that might possibly have extensive implications for cyberspace. The bill does not provide any definition of the term “digital borders”.

It seems that this bill tends to transfer the control of Internet infrastructure from the Telecommunication Infrastructure Company (TIC), which follows policies set by the SCC but operates under the ICT Ministry, to the GSAF. This provision essentially implies that the Supreme Leader will exert control over Internet infrastructure through military oversight. Center for Human Rights in Iran argues\(^28\) that extending such responsibilities to the military can minimize or eliminate any checks and balances - such as parliamentary approval - that the TIC must deal with before it implements policy changes. |
| --- | --- |
| Violations of Net Neutrality | According to Article 19, the ICT Ministry would be required to price the cost of accessing international internet content and bandwidth, as well as access rights to foreign messaging apps, at twice the current rate in Iran\(^29\). 90% of any income that is generated through the sale of international bandwidth would be used to support domestic content and messaging apps.

In another violation of net neutrality, Article 20 requires the ICT Ministry to double the bandwidth of domestic messengers without offering the same to foreign messengers. |
| Online Payments, Financial Services and Cryptocurrencies | Article 21 authorizes online payments through Iranian banks to businesses that operate through domestic messengers. However, similar financial services or facilitating transactions are prohibited for non-state-approved messaging apps (note to Article 21).

Article 23 bans the use and sale of cryptocurrencies through foreign apps but allows for their trade through domestic applications so long as they receive authorization from Iran’s Central Bank. The ICT Ministry would be responsible for blocking any cryptocurrency-related feature of foreign messaging applications. |

\(^{29}\) For more on a similar measure by the ICT Ministry that was proposed in August 2018, see https://www.iranhumanrights.org/2017/12/rouhani-admins-new-fair-usage-internet-price-rates-violate-net-neutrality/.
<table>
<thead>
<tr>
<th><strong>Smartphone Pre-Loading Requirements</strong></th>
<th>According to <strong>Article 24</strong>, all smartphones sold in Iran must also come pre-loaded with domestic messaging apps or they cannot be legally sold. CHRI explains that “this article raises privacy concerns because the pre-sale app installations would have to be carried out by phone producers or vendors who would have to unseal device packages before selling them”(^{30}). The bill provides no further details about who should be permitted to access these personal devices, nor does it offer and personal security guarantees.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Penalties for Unlicensed App Provision</strong></td>
<td><strong>Article 27</strong> penalizes those who (1) “offer” and “launch” messaging apps that are not licensed by the state, and (2) provide services by violating/dismissing the block on unauthorized apps to six months to two years in prison.</td>
</tr>
<tr>
<td><strong>Licensing Requirements for Channel/Group Creation</strong></td>
<td><strong>Article 29</strong> requires a license for creating “channels” and “groups” on domestic and non-domestic messengers. This essentially bans any public activity on messaging apps that is not endorsed by the state. The Ministry of Culture and Islamic Guidance is responsible for passing further regulations with regard to “effective activity” on said platforms.</td>
</tr>
</tbody>
</table>

---

What These Bills Mean

Taken together, these bills contain a number of provisions that should be concerning to digital rights activists in Iran. Although many features of the new legislation are framed either as the delivery of expanded service provision (as in the case of the eGovernment Bill), or to protect citizens’ data from malicious actors (as visible in the Privacy and Data Protection Bill), the proposed legislation poses more challenges than solutions.

We would argue that these bills constitute the foundations of a ‘Filternet 2.0’ – a project that has been the long-term vision of senior policymakers in the Islamic Republic for a number of years.

If in ‘Filternet 1.0’ the Iranian government saw itself as being engaged in a battle to fend off emerging ‘threats’ from the digital world, we would argue that this second phase is marked by the Iranian government’s desire – and increasing capabilities – to play a proactive role in shaping the digital environments and experiences of Iranian citizens, and to covertly influence rather than overtly restrict their engagements with the Internet.

It is our expectation that if these bills pass, we will see an Iranian Internet that facilitates pervasive government data collection; which will be managed by an ever-more complex nexus of unaccountable committees; and which incentivises private tech companies to buy into the state’s system of information controls.

eGovernment Services Enmeshed in the Filternet

During his term, ICT Minister Jahromi has engaged heavily in the development of eGovernment projects and digital service provision. Aspirations for digitalisation are frequently expressed by ICT Ministry officials seeking to explain how the government will be building on the investment in Iranian infrastructure that came with the implementation of SHOMA.

Digitisation and modernisation of Iranian government services is not something that should necessarily be opposed. But the expansion of such services and the roll-out of extensive new data collection and storage practices is something that requires rigorous scrutiny, and the development of data protection standards that are in line with global best practices.

However, on the basis of the draft e-Government Bill, we would argue that the ICT Ministry’s plans could facilitate the introduction of a vast government-led data collection programme that lacks safeguards against abuse.
At the moment, the bill lacks any verifiable commitment to security and privacy for Iranian service users. In light of this fact, it is our concern that limited safeguards exist to prevent Iran's eGovernment program from engaging in dangerous mass data collection practices.

In the absence of such commitments from government, civil society must remain vigilant with regard to the new apps, websites, and technologies deployed by the government and state-affiliated institutions and entities, and seek to audit them where possible.

We would also argue that it is the digital rights community's responsibility to assess the impact of these new government services on marginalised segments of society, particularly those with limited or no access to the internet, who are at risk of being further excluded from government services.

**The Laws Establish Committees, But Few Rights**

The bills currently fail to reform the problematic pre-existing laws governing the Internet in Iran – specifically the 2010 Computer Crimes Law, which is responsible for a whole range of human rights violations. Instead, both the ICT Ministry's bills and the Majles bill propose to establish a whole new host of committees to govern various aspects of Internet regulation – committees that are all too frequently composed of the same players sitting on the CDICC and SCC.

Granting such committees with the authority to set standards and protect the rights of Iranian users will serve as a major barrier to transparency in decision-making processes, and could create the conditions for a further decline in the situation of digital rights in Iran, depending on the eventual composition of these bodies.

If any new committees are established, policymakers in Iran must commit to a much greater level of transparency and reporting than currently exists at the CDICC and SCC.

One of the consequences of the establishment of these committees (likes of SCC and CDICC) is development of a group of Iranian officials to experts on issues of internet policy.

**The Rise of Private Sector Enforcers**

The new bill clearly indicates policy-makers’ ambitions to increasingly deploy the capabilities of the private sector in Iran for oppressing the rights of Iranian Internet users.

The Intermediary Liability Bill, Data Protection and Online Privacy Bill, and Managing Social Messaging Applications Bill all include proposals that
would force private sector companies providing services in Iran to actively participate in the censorship and surveillance regime of Iran.

This could lead to a worrying situation where the survival of new businesses depends to some extent on cooperation with government agencies and complicity in the state's surveillance regime.

**The 2020 Parliamentary Elections Will Matter**

It is unlikely that all of these bills will pass through parliament before the next elections in 2020. In the 2016 elections, reformists ran on a platform that supported the availability of Telegram, but which lacked clear and comprehensive policy pledges related to the internet.

In spite of the fact that the current intake of MPs lacks a coherent position on ICT-related issues, this crowded legislative programme means that the Majles will inevitably have an important role to play in the development of new laws in the coming months and years.

The deputies elected to the next parliament – apart from voting on legislation – will also be the MPs who end up sitting on the quasi-judiciary committees created by this new legislation. As we have seen in the case of the CDICC, the presence of pro-reform MPs on the committee has changed the balance of the committee to the extent that the Judiciary has been unable to rally support for new content filtering on the CDICC.

This relationship with MPs could make these proposed committees something of an unpredictable force in future ICT regulation – representation on these bodies offers an important opportunity for reformist and hardline conservatives currently locked out of the policymaking process to be involved in shaping the eventual implementation of this legislation.

In this respect, parliamentarians aren't just poised to exert influence over the bill's passage, but with the passage of the legislation they may also find themselves empowered to exert more and more influence over the ICT policy sphere in the coming years.
What Comes Next? Potential Threats & Responses

For many Iranian activists, the battle for online privacy, free expression and access to information started in the aftermath of the disputed 2009 presidential elections. At that time, the Iranian state was deploying technological impediments to online expression and access to information. Naturally, Iranian activists and the global digital rights community responded with technical solutions.

As the result of rapid action by technologists and activists over the last decade, it is now widely accepted – even among Iranian officials – that the widespread availability of VPNs has made filtering essentially redundant in large sections of society.

Although in recent years state surveillance has resulted in the arrest, imprisonment – and in some cases, the deaths – of activists and journalists, there is a sense that Iran’s least elegant filtering practices have been defeated. Circumvention tool usage is widespread, and as a result the global Internet remains accessible to large segments of the population.

A large proportion of digital rights abuses are documented, and perpetrators are intermittently held to account – either by international measures (such as sanctions on Iran’s Cyber Police)31, or harsh public opinion (as in conservative presidential candidate Raeisi’s rejection at the polls). During the presidential election 2017, Iranian public and commentators were able to identify Raeisi as one of the officials that during his time at the judiciary he advocated a hard line against digital rights.

Over the last ten years, as the result of activists working on fight back methods and building solidarity to combat filtering regime in Iran there is now an international and formidable network of activists and campaigners making sure that restrictive measures of the Iranian government do not go unchallenged.

However, for the network to be as effective in the next decade we must pay close attention to Iran’s legislative program and the changes it suggests. Only then can we begin to devise solutions to emerging threats – not responsively, but rather pre-emptively.

Building ‘Filternet 2.0’

It is because of all of these victories that adversaries of digital rights in Iran are laying the foundations for what we would call ‘Filternet 2.0’ – or in other words, a ‘Filternet without filtering’.

It is our belief that the slate of far-reaching bills outlined in this report will serve as the fundamental architecture for this new project. Although we anticipate that Filternet 2.0 will largely drop the blunt instrument of content filtering, we expect that this new operating environment will create a host of new risks for citizens and digital rights defenders. For instance:

- **Abuses of digital rights could increasingly go unnoticed by citizens** – As the Iranian government is to expand its online presence through the rollout of eGovernment services and the exercise of greater legal control over private tech companies operating in Iran, it is possible that incidents of censorship or surveillance may become harder to track using existing methods, and that they will be experienced differently by different sections of the society.

- **Content controls and privacy violations could increasingly be implemented by non-state actors in the private sector** – Iran is moving to intensify the support it provides to domestic tech companies responsible for developing domestic apps and platforms. Simultaneously, the slated legislative program looks set to make the private sector an active partner in surveillance and censorship, forcing digital rights activists to reevaluate their technology and advocacy priorities.

- **Increasing convergence between government and the private sector** – Related to our previous point, with the recent developments around domestic messaging apps, a section of the private sector in Iran is becoming increasingly dependent on the government’s protectionist information control measures, which are shutting out major global competitors.

    This emerging consensus between government and many in the Iranian tech sector is particularly dangerous for digital rights activists, with risks of even less transparency and accountability in Iranian information control policy.

Studying Iran’s legislative debates will become a growing priority for digital rights activists in the coming months and years, in order to understand how the government implements the next decade of the Filternet.
Whereas in the absence of a coherent policy agenda our community was forced to use technological measures to glean insights into Iran’s information control regime, we can use the policy debates to start to predict the technological challenges we might face.

More than that, studying the legislative program as outlined this research shows that to insure the free flow of information in Iran and safeguarding the privacy of the internet users in Iran there is a need to develop other solutions in addition to circumvention tools and secure methods of communication.
Credits

Research
Kaveh Azarhoosh
James Marchant

Design
Surasti Puri

Acknowledgements
Small Media would like to thank the contributors to this report who have chosen to remain anonymous. This research would not have been possible without their generous assistance and support.

About Small Media
Small Media is an organisation working to support civil society development and human rights advocacy in the Middle East and Sub-Saharan Africa.

We do this by providing research, design, training, and technology support to partners across the region, and by working with organisations to develop effective and innovative digital advocacy strategies and campaigns. We also provide digital security support to a range of partners to ensure that they can work safely and securely.

This work is licensed under a Creative Commons Attribution-NonCommercial 3.0 Unported License
This bill seeks to develop a coherent regulation of e-transactions. It accredits e-transactions (e.g., commercial and personal transactions) as legal instruments, and validates electronic services offered by state offices. By endorsing and enhancing the scope of e-transactions, the bill also promotes e-government services, and supports new uses of ICTs in commerce and other areas.

The bill sets the rules for electronic mechanisms that state agencies and entities, public and non-governmental bodies, and institutions in charge of public assets and services will use to interact with one another, provide services to the public, and perform other responsibilities.

The bill defines the rights of users and subscribers in relation to service providers. The bill is based on five principles: free and unlimited access to "legal" information, protection of social, cultural, intellectual rights of all individuals, respect to freedom of speech and opinion, protecting security and privacy, promoting ICTs in the society.

The bill on electronic identification seeks to enhance coordination among relevant authorities who regulate and verify electronic IDs. The bill paves the way towards regulating new aspects of ICTs such as online entrepreneurship, Internet of Things (IoT), and domain administration that were not previously addressed in Iran’s legal system.

This bill defines personal data and the parties concerned and elaborates on their rights and responsibilities. It authorizes owners of personal data to directly access or control access to their data at will and within the scope of new regulations.

The bill is designed to address the legal gap in increasingly growing use of foreign social media applications by Iranian citizens. It also seeks to promote use of domestically developed messaging applications at the cost of violating net neutrality and giving clear preference to the traffic that they transfer.
contact@smallmedia.org.uk
facebook.com/SmallMedia
@Small_Media