

Internet Governance

*The quest for an open Internet in the
Middle East and Northern Africa*

Internet Governance

*The quest for an open Internet in the
Middle East and Northern Africa*

Alaadin Al-Radhi • Arash Abadpour • Fahd Btayneh • Fred Andon Petrossians
Rafik Dammak • Mohamed Omran

Policy Review: Hanane Boujemi **Peer Review & Editor:** Rafid Fatani

Proofreading: Cambridge Proofreading LTD
Email: info@cambridgeproofreading.com

Graphic Design: CoCreate Design
www.cocreatedesign.com

Internet Governance: The quest for an open Internet in the Middle East and Northern Africa
Published by the Humanist Institute for Cooperation with Developing Countries (Hivos)

Creative Commons Attribution 3.0 Licence
<creativecommons.org/licenses/by-nc-nd/3.0/>
Some rights reserved.

CONTENTS

<i>PREFACE</i>	<i>7</i>
----------------	----------

<i>EXECUTIVE SUMMARY</i>	<i>10</i>
--------------------------	-----------

<i>EGYPT</i>	<i>11</i>
INTERNET OPENNESS	12
IMPORTANT ASPECTS OF THE INTERNET LEGISLATIONS AND POLICIES	13
INTERNET FREEDOM OF EXPRESSION: CHALLENGES AND LIMITATIONS	14
INSULTS TO THE MILITARY INSTITUTION	14
INSULTS TO RELIGIONS	15
ACCESS TO INFORMATION IN EGYPT	15
TRANSPARENCY AND ACCOUNTABILITY	16
E-PARTICIPATION	17
THE IMPACT OF SOCIAL MEDIA ON CIVIL LIBERTIES	17
FILTERING	19
CONCLUSION	21

<i>IRAN</i>	<i>22</i>
LAWS AND COMPUTER CRIMES	22
NATIONAL INTERNET: A “FILTERED” WORLD WIDE WEB	23
FILTERING: AN EVERLASTING PROBLEM	25
REPRESSION: VIRTUAL WRITERS, PHYSICAL VICTIMS	26
INTERNET CONTROL TECHNOLOGY	28
ACCESS TO INFORMATION	28
E-GOVERNMENT	30
THE IMPACT OF SOCIAL MEDIA ON CIVIL LIBERTIES	31
CONCLUSION	33
RECOMMENDATIONS	34

<i>IRAQ</i>	36
EXECUTIVE SUMMARY	36
INTERNET BACKGROUND IN IRAQ	37
CURRENT SITUATION OF INTERNET OPENNESS IN IRAQ	38
ACCESS TO INFORMATION STATUS IN IRAQ AND E-PARTICIPATION	39
IRAQI INTERNET LEGISLATION, POLICY, REGULATORY ENVIRONMENTS & FRAMEWORKS	39
IRAQI CHALLENGES, BARRIERS AND LIMITATIONS	40
CONCLUSIONS	42
RECOMMENDATIONS FOR THE WAY FORWARD	43

<i>JORDAN</i>	44
FREEDOM OF EXPRESSION (FOE) AND THE CURRENT SITUATION OF INTERNET OPENNESS	45
NICHES OF AREAS OF IMPORTANCE WITHIN THE INTERNET LEGISLATION/POLICY	47
STATUS OF ACCESS TO INFORMATION, TRANSPARENCY, ACCOUNTABILITY, AND E-PARTICIPATION	48
THE IMPACT OF SOCIAL MEDIA ON CIVIL LIBERTIES	49
CONTENT FILTERING	50
CONCLUSION AND RECOMMENDATIONS	51

<i>SYRIA</i>	53
INTERNET OPENNESS	53
INTERNET LEGISLATION AND POLICY	54
FREEDOM OF SPEECH ON THE INTERNET IN SYRIA: CHALLENGES AND LIMITATIONS	55
ACCESS TO INFORMATION	56
TRANSPARENCY AND ACCOUNTABILITY	57
E-PARTICIPATION	57
THE IMPACT OF SOCIAL MEDIA ON CIVIL LIBERTIES	58
CONTENT FILTERING	59
RECOMMENDATIONS FOR POLICY MAKERS	59

TUNISIA

61

THE INTERNET: BETWEEN THE STATUS QUO AND CHANGE

62

OPEN GOVERNMENT: NEW OPPORTUNITIES AND POSSIBLE PITFALLS

63

CONCLUSION

66

RECOMMENDATIONS

66

PREFACE

The emergence of the Internet into our daily lives has radically altered the consumption, production and distribution of information, and has already played an influential role in shaping political systems. Knowing no traditional geographic, legal or political boundary, the Internet has largely shaped its own culture and its complex reality challenges traditional perspectives on the role of governments and the importance of boundaries and sovereignty. However, Internet governance mechanisms should be based on the principle of openness, encompassing tolerance and freedom of expression. These mechanisms, together with unilateral policymaking could potentially hinder the free flow of information on the Internet.

The ongoing uprisings in the Middle East and North Africa (MENA) have unsettled the political dust in what is already a very fragile region. As an enabler of human rights, the Internet has helped mobilise social movements to impact on and improve political surroundings in ways which had not previously been possible. Although some downplay the significance of the Internet in the ongoing revolutions, there is no doubt regarding its paramount role in facilitating the sharing of information and of mobilising people on the ground during the height of the uprisings.

Tunisia and Egypt saw first-hand how such ability to share information online proved vital to their revolutions and how the Internet contributed to

the downfall of the governments of both countries. However, this was not the case in Iran where the regime's fear of Internet technology has led to a hard-line policy on Internet technology and to further social and political depravation.

Because freedom of expression and the free flow of information and knowledge are essential to democratic societies, the focus of this publication is on helping to advance human rights and democracy. It compiles the experiences of six politically fragile countries from across the MENA region – Egypt, Iran, Iraq, Jordan, Tunisia and Syria - in reports from selected experts in the field. These experts have collected, analysed and synthesised up-to-date data from a variety of sources including domestic and international human rights organisations, governmental sources, non-governmental organisations and members of civil society in their respective countries. Once the reports had been drafted, they were rigorously edited, reviewed, and fact-checked so as to ensure accuracy and objectivity.

This method contextualises each country's experience of anchoring and safeguarding Internet openness. In the context of this report, Internet openness consists of the policies and measures which permit Internet users to make their own choices about which lawful Internet services and content they wish to access, create or share online. Whilst at first glance the six

reports appear to be similar, their contexts and analyses are diverse and each has a different implication for social mobilisation using the Internet. The present article will explore these issues in detail.

THE BREAKDOWN

Each country's report is loosely structured around two sections. The first is focused on Internet openness at the local level. Each expert highlights how freedom of expression is understood in their national socio-political context and the legal provisions which limit or regulate freedom of expression in that country. They then address issues including freedom of speech on the Internet in their country, challenges and limitations to that freedom of speech, access to information, how much transparency and accountability is reflected in the policy-making process and beyond. The experts also assess whether or not, and to what extent, e-participation plays a role in political activity, together with the impact of social media on civil liberties, and Internet governance issues unique to their country.

The second section analyses the role of civil society. This includes identifying local and regional civil society networks involved in Internet governance, their role in the policy-making processes, the extent to which they influence local Internet policy and the extent to which online communication is secure. This section also identifies different governmental bodies and businesses involved in Internet legislation and governance.

THE POLICY-MAKING PROCESS

Whilst the reports do not consider physical access to technology, the legal, policy and regulatory frameworks are explored in detail in order to identify issues surrounding the safeguarding of Internet openness. National-level Internet governance varies between states, most notably with respect to the roles of government, civil society, the private sector and other stakeholders in both policy-making and governance. In some countries, Internet management at national level is in the hands of governments and regulators, whilst other countries allow private and non-for-profit sector involvement together with other stakeholders.

Although still fairly small, awareness is growing amongst regional civil societies regarding how to influence national Internet policy, and pressure on MENA governments to adopt progressive legal mechanisms continues to strengthen. Five of these six reports indicate that the policy-making and legislative process and environment do not take a multi-stakeholder approach and do not engage civil society. This has a knock-on effect on the safeguarding of Internet openness. Whilst Tunisia is an exception, it is nonetheless in the early stages of developing a multi-stakeholder policy-forming process and still has some distance to go with regard to increased inclusion.

COMMON LANDSCAPE

A consistent feature of all six reports is the lack of transparency in governmental administrative procedures, even when ICT facilities and infrastructures are available. This translates into

a lack of a coherent ICT socio-political vision, which inevitably encourages arbitrary ICT policy environments.

Another common theme is the way in which lack of transparency in facilitating access to governmental and economic decisions has excluded citizens from taking part. This said, all six states have rolled out e-government programmes, some of which have been more effective than others.

An additional challenge facing online communities and activists relates to the violation of individual privacy and legal threats based on online activity. Consequently, another universal theme is the ambiguity and vaguely-worded nature of Internet legislation. Such laws prompt citizens to self-censor content in the fear of detention on unclear grounds. The Jordanian report highlights cases where this has hindered Internet openness.

The fact that the Internet does not adhere to geopolitical boundaries poses a serious obstacle to governments seeking its over-regulation, and this in turn poses a threat to Internet openness. A core principle of the Internet is that it should be free and universal, thus meaning that over-regulation cannot be a good thing.

RESTRICTIVE CONTENT

Internet content censorship is common in the MENA region. However, governments have not been able to silence activists and human rights advocates because of the technical evolution of

online platforms and applications. Despite this, governments have employed innovative tactics to censor and restrict access to content. These have included slowing bandwidth speeds and limiting the ability of users to upload or download content such as videos or images. With the exception of Tunisia which has transitioned from filtered to unrestricted Internet, the six countries in this publication have limited Internet access through physical and technical infrastructures.

Whilst most of these governments aim to restrict access to content, these six countries have developed a range of approaches to Internet regulation and have been met with varying degrees of success, sometimes with unintended consequences.

CHALLENGES FACING ACTIVISTS

International companies have provided technical surveillance and monitoring systems to the governments of all six countries. Such systems enable national security apparatuses to violate privacy and monitor Internet activities without consent and due diligence. In so doing, these European and North American companies have assisted the governments in detaining political activists and human rights defenders. This interrupts the work of civil societies and activists towards securing human rights in their respective countries.

EXECUTIVE SUMMARY

Many have often criticised attempts by traditional governing bodies to regulate the Internet. They believe that any regulation goes against the openness philosophy of the Internet. However, whilst the Internet is not under the responsibility of any official government, it can be governed by the social norms of its users, as well as by national governments in a more explicit manner. These social norms to which the users are subject, can be influenced by national legislation or procedures, and also by cultural and economic trends which indirectly shape Internet users' choices and patterns online.

The ongoing unrest in the Middle East and North African (MENA) region has opened up new debates on the Internet's openness and the role it plays in development and democracy. The report strives to analyse the current state of Internet openness in six countries; Egypt, Iran, Iraq, Jordan, Tunisia and Syria - from hand selected experts in the field. The reports contextualise each country's experience of anchoring and safeguarding Internet openness, including policies and measures which permit Internet users to make their own choices about which lawful Internet services and content they wish to access, create or share online.

Whilst the report considers the prospects of openness in the six selected countries in the same region, it finds that they are very mixed in positions: despite the fact that Tunisia, at one end, is on track to achieve positive political

reform which has been an enabler to Internet openness in the country, Syria is experiencing profound internal division and conflict which has fuelled the current regime to further limit Internet access to its citizens. In Egypt, which epitomizes many regional trends, protection of Internet openness has been limited due to the Islamist movement taking control following the fall of the former Hosni Mubarak regime. Jordan has found some reform encouraged by the regime's necessity to boost economic growth, although red-lines seem to creep behind citizens using the Internet. In Iraq, the overthrow of the dictator Saddam Hussein's regime in 2003 was a milestone, but has since led to chaos and the inevitable limiting of Internet openness amidst fear of further public disturbance. Finally the Iranian regime's apprehension of toppling like some of its neighbours has resulted in paralysing authoritarian policies which limit citizens' Internet use for social and economic development.

EGYPT

“The Facebook Revolution” is a name popularly given to the Egyptian uprising of 25 January 2011. The use of the term ‘Facebook’ refers to the major role the Internet and social media played in the success of the revolution, the main slogan of which was “Bread, freedom, social justice”. Both before and after the uprising, it provided a vital opportunity for Egyptian youths to evade censorship and control and express themselves freely and independently.

Whilst these freedoms began in virtual space, they were quickly replicated in the real world at Tahrir Square in Cairo. However, freedoms of expression won after the revolution have not been immune to destructive setbacks for both political and religious reasons. It has been argued that the concept of ‘freedom’ has not yet been fully developed amongst Egyptians. This is due to historical political and faith-based conflicts, which have permitted a number of public and individual freedoms, including the freedom of expression, to be restricted and threatened by attacks and violations.

Following the revolution, Egypt has been going through a period of legal and constitutional vacuum.¹ The Supreme Council of the Armed Forces (SCAF) was in charge of governing the country after the toppling of the old Hosni Mubarak regime. On 19 March 2011, the SCAF

began a referendum on constitutional provisions, which in turn led to the Constitutional Declaration of the Republic of Egypt. This Declaration has since been amended four times: three under the rule of the SCAF and a fourth time under the rule of the current president Dr. Mohammed Morsi - candidate of the Freedom and Justice Party (FJP), the political arm of the Muslim Brothers. These amendments reflect the political, constitutional and legal chaos in Egypt during the democratic transition period and the construction of the so-called ‘Second Republic’.

Although freedom of expression is guaranteed by Articles 12 and 13, as amended on 17 August 2012² of the Constitutional Declaration, the Declaration also permits “constructive self-criticism to ensure the safe construction of the nation” and excludes the State of Emergency. This means that laws restricting freedom of publication are still in force. Freedom of expression is also subject to many restrictions in the Penal Code² and the Communication Code No. 10-2003.³

During the period of SCAF rule, with an Islamist majority in Parliament, many bloggers, journalists and freedom-of-expression activists were restricted and arrested. They were accused of disturbing public order, libel, defamation and

1. See statement by The Forum of Independent Human Rights Organizations <http://www.cihrs.org/?p=3004&lang=en>

2. Articles (80, 95, 98, 171, 179, 181, 182, and from 184 to 187, and from 189 to 198, 302, 303, 308, 309) The Egyptian Penal Code is also available at <http://goo.gl/AoiX>

3. Articles 44, 64, 65; 66. The laws regulating communication are available at the following link <http://right2know.afteegypt.org/index.php?newsid=32>

campaigning against the military forces. This situation did not change when the elected president took office. During the first 100 days of his rule accusations were made of insulting the president, Hisba cases (contempt for religion) were brought, whilst journalists and media professionals were also arrested. In addition, there have been restrictions on artists and the creative community, whilst sit-ins have been ended by force, and numerous assaults have been reported.⁴

INTERNET OPENNESS

According to the Egyptian Ministry of Communication and Information Technologies (MCIT) the estimated number of Internet users in 2000 was 450,000 with a growth rate of 16.93% per year. This number is now estimated at 31 million and reflects policies under the former regime which sought to benefit economically from expanding the Communications and Internet sector. Following the emergence of third generation GSM phones in 2005, Blackberry service and smart phone usage increased the number of mobile Internet users to 10,780,000 in 2013 – equating to 35.02% of Internet users in Egypt. The number of users employing USB modems has increased by the same amount and is today estimated at 3 million.⁵

After the political, economic and cultural effectiveness of the Internet and social networks became apparent, 2002 saw the ousted regime attempt to sharpen its profile in information and communication technologies by the Ministry of the Interior establishing a cybercrime office. Its role was to control Internet activists and to confiscate equipment in the absence of legal provisions. Many citizens were tried for deviance and the dissemination of false reports.⁶

When the revolutionists raided the State Security Police offices in March 2011, documents were found which revealed that the police cooperated with the American Company JAMA, using the spy software FinFisher. JAMA also trained police officers to use the software to tap phones and monitor VOIP Internet conversations. This spy software can use computer cameras and mobile phones for eavesdropping and control.⁷ In the absence of clear laws the government often censored sites without following judicial processes.

Internet Cafés complained about excessive police control when they were required to photocopy the IDs of Internet users, asked to monitor any sites used and submit reports. Another tactic was the use of prepaid cards in tourist-class cafés which would send a password to mobile phones.⁸ The number of Internet cafés

4. See the report of the Arab network for Human Rights -Freedom of Expression in Egypt: Expression after Election of a Civil President. <http://www.anhri.net/?p=60153>

5. Source: Ministry of Communication and Information technologies-Briefing on Communication and Information technologies Indicators, August, 2012. Monthly issue, at http://www.mcit.gov.eg/Upcont/Documents/Publications_1992012000_Eng%20Flyer-August2012-last.pdf

6. Study by the Arab Network for Human Rights, Internet in the Arab World : Implacable Adversaries: Arab Governments and the Internet' <http://www.anhri.net/en/wp-content/uploads/2012/02/Implacable-Adversaries.pdf>

7. Jamie Doward, « Crackdown on sale of UK spyware over fears of misuse by repressive regimes », the Guardian, available at <http://www.guardian.co.uk/world/2012/sep/09/block-on-exports-surveillance-equipment>

8. Study by the Arab network for Human Rights, Internet in the

decreased drastically because of the increased use of WiFi and USB Modems whilst many were turned into electronic games and entertainment rooms.

IMPORTANT ASPECTS OF THE INTERNET LEGISLATIONS AND POLICIES

Some of the major violations committed by the former Mubarak regime during the uprising included instructions to ICT operators and ISP's in Egypt to cut off all forms of communication.⁹ As a result there was no service for three days, no Internet connection for five days and none of the injured were able to contact medical rescue services for help.¹⁰ This action was based on articles 65 and 67 of the Sixth Part (National Security and General Mobilization) of the Telecommunication Regulation Law 10-2003).¹¹ The same law, in Part One, Article 1, Paragraph 20 (General Provisions) defines national security in the following terms: "It includes the Presidency of the Republic, the Ministry of Interior and the National Security Committee and the National Administrative Control Committee."

This definition involves many parties with

different responsibilities. It can be argued that it does not provide for restrictions on the decisions of such committees, although there should be a clear responsibility at the very top of State authority. On its website, the MCIT published that the fifth plan 2012-2017 is concerned with the development of a legal framework for ISP's and information technologies. It also proposes amendments to the existing laws including law 10-2003 which regulates communication. However, the proposed amendments to Article 55 of the law¹² came without review, nor was there a redefinition of the role of the national security apparatus in regulation. The proposed amendments also failed to include Articles 65 and 67 where provisions are related to the suspension of communication services. This is allowed entirely or partially in specific cases involving general mobilization such as a state of war or in the event of tensions with other States and crises threatening national security. The events of 25 January were considered a threat to national security.

MCIT included the legal environment regulating communication and information technologies in its five-year plan and raised the issue of regulating the communication sector. One law amended by the committee was the Telecommunication Regulation Law N° 10-2003 and the law on Electronic Signatures N°15-2004. It also submitted drafts for new laws such as the law on the Dissemination of Data and Information, the law on Cybercrime, and the law

Arab World : Implacable Adversaries: Arab Governments and the Internet' <http://www.anhri.net/en/wp-content/uploads/2012/02/Implacable-Adversaries.pdf>

9. <http://web.archive.org/web/20110324202228/http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml>

10. See statement by the Arab Network for Human Rights against the minister of communication and the three GSM operators for the killing of protestors <http://qadaya.net/?p=918>

11. These provisions give broad powers which allow the security forces to control communication, the Internet and providers of such services in case of general mobilization and national security? These provisions are available at: http://www.tra.gov.eg/uploads/law/law_en.pdf

12. National Strategy for Communication and Information Technologies 2012-2017 (The Egyptian Digital Society and Knowledge Economy) pages 32 till 37 <http://www.mcit.gov.eg/Upcont/Documents/ICT%20Strategy%202012-2017.pdf>

on Electronic Trade.¹³ However, current drafts still require revision as well as consultation with stakeholder groups.

INTERNET FREEDOM OF EXPRESSION: CHALLENGES AND LIMITATIONS

Freedom of expression within societal and constitutional terms is subject to restrictions and challenges and still faces an uphill struggle. It is constantly being undermined both legally and socially. Despite the majority of provisions for freedom of expression being rather good, the current Constituent Committee with a majority from the Islamist Party is insisting on compliance with their interpretation of Islamic laws. This constitutes a significant threat to the liberties provided in the draft Constitution. Whilst the Egyptian Constitution defends followers of the revelation religions (ie, Islam, Christianity, and Judaism) it may represent a threat to other faiths. During the interim SCAF rule, military prosecution and court martial were used against civilians and it became clear that Egyptian criminal law can pose a potential setback when used to punish contempt for religions in Article (98v)¹⁴ and that it can also be used against Internet activists and users.

13. Op. Cit.

14. Article 89 of the Egyptian Penal Law, 'shall be imprisoned for no less than six months and no more five years and a fine of no less five hundred pounds and no more than one thousand pounds, anyone using religion for the dissemination for or campaigning for, in writing or any other means, radical ideas the aim of which is causing disputes, discontent to any of the revelation faiths or followers of any of their schools and which may affect national unity and social peace ».

INSULTS TO THE MILITARY INSTITUTION

The activist Michael Nabil, the first freedom-of-expression victim of the recent Egyptian revolution, was accused of insulting military forces through publications on his personal social media accounts (Facebook -Twitter). In his blogs "Son of Raa" and "The Army and the People wasn't ever one Hand"¹⁵ he rejected the excessive use of violence against protesters in Tahrir Square and opposed mandatory military service. He was detained in his house in Cairo on 28 March 2011, and sentenced to three years' imprisonment on 10 April 2011 following which he was subjected to extremely bad conditions in both legal and medical terms. On appeal, his sentence was reduced to two years and on 2 January 2012, the SCAF said it would offer him amnesty, together with over 2000 other detainees sentenced by military courts on the occasion of the first anniversary of the revolution.¹⁶

On 13 August 2011 the Egyptian activist Asmaa Mahfouz, the former woman leader of the 6 April movement, was summoned for interrogation by the military prosecutor. She was interrogated for over three hours regarding comments she posted on Twitter and for the publication of interviews in which she criticized the army for failure to protect protestors. On 16 August an army official told the Middle East News Agency that the prosecutor referred Mahfouz's case to the court

15. See article 'The Army and the People wasn't ever one Hand' on the blog of Michael Nebil, available at: <http://www.maikelnabil.com/2011/03/army-and-people-wasnt-ever-one-hand.html>

16. See statement by Amnesty International on the liberation of Michael Nabil on 24 January 2011. <http://www.amnesty.org/en/news/egypt-release-blogger-maikel-nabil-end-cruel-ordeal-2012-01-24>

for prosecution because of accusations involving insults to the army, while other accusations were not held against her. Mahfouz told Human Rights Watch that the accusations were withdrawn on 18 August 2011.¹⁷ She also faced accusation for a Tweet stating “the Abassia people say that Rowini and Tarek Zaydan had been in the street in the morning and said there was a protest of rogues who would fight the army”. Tarek Zaydan, the president of the Revolution Party, accused her of false accusations but the court dismissed her case on 6 May 2012.¹⁸

INSULTS TO RELIGIONS

Since 25 January 2011 accusations for content involving religious insults published on private social network accounts have increasingly been used by Islamist movements against political activists and bloggers. These began with an accusation against the businessman Naguib Sawiris for a tweet on his Twitter account in which Mickey Mouse wears a long beard and Minnie Mouse a Niqab. Sawiris’ case was dismissed by the court.¹⁹

In the aftermath of the crisis engendered by the film “Innocence of Muslims”, the public prosecutor accused the activist and blogger Alber Saber Ayad of insulting religion when he published a link to the film on his Facebook

page. He was followed and physically assaulted in Cairo’s Marg police station, before being taken to court. His family were forced to leave their house following death threats and threats to burn down their house.²⁰ Ayad was sentenced to 3 years in prison and was presented with a 1000 L.E fine by El Marg court.²¹

ACCESS TO INFORMATION IN EGYPT

Article 47 of the 1971 Constitution²² states that:

“the right of access to information shall be guaranteed; every citizen shall have the right to freedom of expression, of speech, of opinion, in writing or photography or other forms of expression within what is permitted by the law, self-criticism and constructive criticism as a guarantee for the safe construction of the nation.”

Freedom of expression and opinion is regarded by both the Fiqh and the law as the mother of all freedoms. However, Article 47 does not provide for the freedom to disseminate information in an overt way.²³ The 2011 Constitutional Declaration also does not include the right of journalists to access information, as was the case in the 1971

17. See statement by Human Rights Watch ‘Egypt one Year of Aggression against Freedom of Expression’, at <http://www.hrw.org/news/2012/02/11/egypt-year-attacks-free-expression>

18. See statement of the Arab Network for Human Rights ‘Rule benefiting activist Asma Mahfoudhi in a Twitter case is a new victory for freedom of expression and an opportunity to review the Penal Law’ <http://www.anhri.net/?p=52826>

19. See statement by Human Rights Watch ‘Egypt one Year of Aggression against Freedom of Expression’, at <http://www.hrw.org/news/2012/02/11/egypt-year-attacks-free-expression>

20. See joint statement by the Association for Freedom of Thought and Expression and Center to Support Information Technologies <http://www.afteegypt.org/pressrelease/2012/09/30/718-afteegypt.html>

21. See the joint Statement by 11 Egyptian Human Rights defender organisations “ The prison sentence against Alber Saber: another nail in the coffin of democracy” at: <http://www.en.afteegypt.org/index.php?newsid=108>

22. See the Arab republic of Egypt 1971 constitution http://www.sis.gov.eg/en/LastPage.aspx?Category_ID=208

23. See study by Association for Freedom of Thought and Expression (AFTE) “legal study on freedom of exchange of information” <http://www.en.afteegypt.org/index.php?newsid=83>

Constitution. This is a regression, as the right to disseminate information must be protected in major legislation such as the Constitutional Declaration.²⁴

According to Article 41 of the draft published on the website of the Constituent Assembly on 14 October 2012:

“free access to information and data (statistics and documents), regardless of its place and origin, shall be a right guaranteed to all citizens, the state shall enable them in the practice of this right without impediments as far as this does not conflict with national security or breach privacy. The law shall provide the regulations for obtaining information, or in cases of complaints in case information is denied and providing the appropriate sanctions to anyone who denies such a right.”

In the absence of a clear law in previous Egyptian Constitutions, the recognition of this right is a positive step forward. However, despite the law being applicable to everyone in accordance with international laws on human rights, this Article appears to exclude foreigners.²⁵

MCIT promised to support “the law to provide information and data.” According to the ministry, it is a comprehensive law made up of seven chapters and fifty Articles. The Legislation and Laws Committee opted to follow the European school and established a ‘Higher Data and Information Council’.²⁶

24. Op.Cit.

25. See the draft constitution at http://dostour.eg/dostor_masr.pdf

26. Source, National Strategic Study on Communication and Information technologies 2012-2017 (The Egyptian Digital Society

TRANSPARENCY AND ACCOUNTABILITY

At governmental level, Egypt suffers from an absence of transparency and accountability. According to Transparency International, Egypt ranked 118 out 176 countries, scoring 2.9 out of 10 possible points where each point relates to a specific criterion.²⁷ According to the MCIT, the next five-year plan will include publication policies, making information accessible by providing appropriate legislation, improving the opportunity to provide public information and data on the Internet in electronic versions, and providing and developing mechanical means for the attribution of authorizations to use national data and information on the Internet.²⁸

Using private initiative, a website dubbed Morsi Meter was established to monitor the performance of the first post-revolution elected civil president during his first 100 days of office. Monitoring was based on what he himself had promised to achieve in that time and was conducted using media for all issues relating to Morsi’s declarations - namely security, food, property, traffic and energy, as well as statements and declarations made by the President.²⁹

Within the framework of contributions by civil society organizations, three NGOs submitted a draft law for the Dissemination of Information.³⁰

under the Knowledge Economy) July 2012 http://www.mcit.gov.eg/Publication/Publication_Summary/660/ICT_Strategy_2012-2017

27. See Transparency International, Corruption by country http://www.transparency.org/country#EGY_DataResearch_SurveysIndices

28. Source, National Strategic Study on Communication and Information technologies 2012-2017 (The Egyptian Digital Society under the Knowledge Economy) July 2012 http://www.mcit.gov.eg/Publication/Publication_Summary/663

29. See <http://www.morsimeter.com/en>

30. See draft law submitted by (Egyptian Personal Rights

They insisted that it is essential to improving both the performance of the State apparatus and government as stakeholders and the investment climate - to protect investment opportunities in a transparent environment so that appropriate decisions can be based on real facts. The project highlights the duty of government structures to spontaneously provide a maximum amount of information on the Internet in order to reduce applications to obtain it. It also highlights the possibility of obtaining information through searches on the Internet.

E-PARTICIPATION

It is possible to say that e-democracy in Egypt is better than e-participation and this will be clarified further in the following section. Egypt has e-participation tools such as websites, blogs, social networks and wikis. However, participation mechanisms and tools are still limited; for example, Egypt does not have an electronic voting system. Governmental e-services are either very limited or absent. They provide information but no services and most links are not fully functional. Such limited facilities have led to Egypt being ranked 107th globally in terms of e-governance.³¹

The MCIT is currently working on the amendment of laws involving issues such as e-signature. It is also working on a draft law regarding cyber security. Since it no longer faces past obstacles such as the lack of computer equipment, low

Internet usage and poor computer and Internet literacy, its five-year policy plan also aims to develop electronic identities and to connect government services, which would help improve the performance of e-governance.³² Connecting Ministries through a national Intranet would help provide data and information rapidly and develop large-scale mechanised and secure databases.

The logo of the website of the Constituent Assembly is “The people write their constitution”.³³ It provides a forum for the discussion of constitutional provisions through a website accessible to citizens. It also publishes minutes of the meetings and plenary meetings of the Assembly. This saw the withdrawal of a large number of representatives from civil society and most who remained came from religious backgrounds. The electronic committees - an arm of these movements - were able to orient discussions towards a single major goal. The blogger Kareem Amer complained on his personal Facebook page that his website comments had been removed. Discussions were chaotic as the material changed rapidly and the draft website Constitution was modified several times.

THE IMPACT OF SOCIAL MEDIA ON CIVIL LIBERTIES

E-democracy in Egypt developed in a very visible way, and has impacted heavily through social networks (Facebook and twitter) and live streaming websites (Bambuser, You Stream) as

Initiative, Freedom of Expression and Thinking Foundation, support to information technologies) <http://eipr.org/en/pressrelease/2012/03/01/1396>

31. See UN Report “E-government Survey 2012: E- Government for the people” <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf>

32. Source, National Strategic Study on Communication and Information technologies 2012-2017 (The Egyptian Digital Society under the Knowledge Economy) July 2012 http://www.mcit.gov.eg/Publication/Publication_Summary/663

33. See official Constitution Association website <http://dostour.eg/>

well as video and photo sharing sites (YouTube, Daily motion, Flickr). It is because of these networks that the revolution has been called the Facebook or Internet revolution.

In light of political restrictions on the right to peaceful protest and the tight grip of the State on established media outlets, blogs have increasingly focused on political discourse. The names of a number of bloggers soon became associated with their political activism and harsh criticism, while cultural, art and literary blogs regressed. In 2004, prior to the 2005 Constitutional amendments which led to presidential and parliamentary elections, the Kefaya movement emerged. It was behind blogs which supported political and human rights activists against the oppression they faced. “*Egyptian Awareness*,” a blog by Wael Abas and “Alaa and Manal,” emerged and started developing websites such as the *Kefaya* website. The first test of the new media was the call, on Facebook, for a strike on 6 April 2008. While the established media obscured events, both Facebook and Youtube covered the strike, and social and participative media were very successful in mobilizing the masses and organizing related events.

Well-established bloggers launched a youth training campaign on the use of the new media in such mobilisation and organization. A global campaign was put together and legal support made available with the emergence of the Front to Defend of Egypt Protestors, which developed its tools using the new media. A Campaign to Defend Egyptian Students and Campaign 21606 to fight low wages, were also launched. The opportunity to use live social media tools was seized upon, thus giving a new dimension to the democratic transition.

Social media also played a leading role in unveiling a number of cultural issues such as sexual harassment (Aid Fitr 2007), torture in police stations and prisons (Emad El Kabir) and corruption (the ferry case). This made possible the flow of information in an unprecedented way. Young people overcame the barriers of virtual transmission to meet on the ground, while the virtual world remained a support to their activities.

New media have been used in monitoring the first presidential and parliamentary elections in 2005 through bloggers taking photographs and videos involving alleged election-rigging, violence and militia action. News published on blogs and social networks was later used in the Referendum for the Amendment of the Constitution and the experience and skills acquired were later used in monitoring the 2010 elections. The emergence of new social networks had a huge impact on coverage of the elections as the concept of people’s watch gained momentum. Many civil society organizations (the Independent Alliance of Monitoring the Elections, the Egyptian Association for the Support to Democratic Development, and the Egyptian Democracy Institute) used social networks to monitor events. Electoral observers, who documented and monitored the elections, benefited from training on how to use the digital tools at their disposal, such as mobile phones, digital camcorders and laptops.

The emergence of Dr. Mohammed Baradei as a virtual presidential candidate gave huge impetus to Egyptian politics. He was supported by a large number of the youth population who mastered new information technologies. The new media were used to establish contact with Internet

users, on social networks such Facebook, Twitter and YouTube. Many of those involved in the campaign were subject to police harassment.

When a young man - Khaled Saeed - died from physical assaults by the police in the streets of Sidi Gaber in Alexandria, a Facebook page, "*We Are All Khaled Saeed*" was created. Its members numbered hundreds of thousands within a week and went on to exceed two and a half million. The page called for a protest to oppose torture on 25 January 2011 (Police Day in Egypt). The page also reported the death of Sayed Belal, the second death at the hands of Alexandria police - one of the sparks which ignited the 25 January revolution, and another reason why it has been called the Facebook revolution.³⁴

As it was aware of the role of the new media and social networks, SCAF created a Facebook page on which it published statements and declarations. Official media reported to the public from statements made on the page. With increasing violations and violence of the Council against protestors and rebels and the number of those put on trial by military courts, other pages emerged. "*No to Military Trials*" and "*Military Liars*" documented events and published on social networks. Documented violations formed part of a road show and protest events on the streets of Egyptian cities.

Just as new media contributed enormously to the consolidation of civil, economic, social and cultural liberties, they have also contributed to the polarization of Egyptian society in the light of an emerging democracy where difference is

still not tolerated. Electronic commission, made mainly by members of the dissolved part and the Muslim Brotherhood³⁵ has contributed radically to the polarization process.

FILTERING

The Internet is free in Egypt, but Internet users are not. The Egyptian governments have not forbidden or censored websites; they have simply blocked them before allowing them to resume, often on the same day. The only exception to this was the People's Party website in the 1990s. Since then the government has censored or filtered Internet content only during the revolution, precisely on 25 January 2011 when access to five sites was blocked (Facebook Twitter, Bambuser, and the sites of two newspapers Al Badil and the Dostour). The government lifted the ban on all sites except the Dostour newspaper on 26 January 2011.³⁶ However, Internet connection was not available again on the morning of the 28 January. Connection was suspended for five full days.

On 7 November 2012, the General Prosecutor ordered the censorship of Internet pornography sites and a regulation to filter immoral content which may be considered contrary to Egyptian traditions, values and the sovereign interests of the country.³⁷ The court ruled in May 2009 that

34. See Introduction of the National Coalition for Media Freedom 'The New media and its Role in supporting the Popular and Political Participation Mr. Mohammed Omrane <http://ncmf.info/?p=204>

35. Article on Jadaliyya website by authors Linda Harira and Mark Lotfi, "The Muslim Brothers' E-Militias: How to Upload Ideology on Facebook". http://arabic.jadaliyya.com/pages/index/7212/e-militias-of-the-muslim-brotherhood_how-to-upload

36. See press release of the Arab Human Rights Network, 'Continuous Censorship of Dostour Site. The Arab Human Rights Networks condemns the attempts of the government to censor protests demanding democracy,' 27 January 2011, at <http://www.anhri.net/?p=23294>

37. BBC at <http://www.bbc.co.uk/arabic/>

the MCIT censors such sites because of their impact on religious and moral values. However, this decision was not enforced because the Ministry found they were difficult to identify.

After the revolution, the Administrative Court issued a ruling on 30 March 2012 to 'censor pornographic sites'. The Court ordered the Minister of Communication and the President of the National Communication Commission to enact this censorship. The Lawyer Abulaziz Ibrahim Ourabi turned the Courts against the Prime minister and the Minister of Communication by asking for the censorship of such sites. The Transport and Communication Commission of the dissolved parliament submitted a request to censor pornographic websites in a request submitted by the Nour Party member, the Salafist Younes Makhion. The report mentions that "Egypt is facing assaults by these sites which are more dangerous than any enemy."³⁸

The US film 'Innocence of Muslims,' deemed by many to be a direct insult to Muslims and Islam, triggered a wave of global protests. These protests started in front of the American Embassy in Cairo, which was later invaded by protestors. That evening, protests spread to Benghazi in Libya where they escalated into an armed attack using heavy artillery against the American Consulate, thus leading to the death of the American ambassador to Libya. A number of embassies in Arab and Islamic states were subsequently attacked. In Egypt, protestors demanded the censorship of the film on YouTube; the demand was rejected by Google.

middleeast/2012/11/121107_egypt_porno_sites_web.shtml

38. CNN Arabic at http://arabic.cnn.com/2012/middle_east/3/30/Egypt_Enetnet/ accessed on 18 October 2012 at 03:18 p.m.

However, following popular protests and global lobbying, Google censored the film in several countries (Egypt, Libya, Saudi Arabia, Indonesia and Malaysia).³⁹

When the film was shared on Egyptian social networks, a lawsuit was filed in September 2012 by Egyptian attorney Hamed Salem. Hundreds were injured in Egypt and on 9 February the administrative Court ordered the ban of YouTube for a month for failing to remove the film. The Court verdict also applied to any website which aided in the sharing of the 13-minute film.⁴⁰ However, on 14 February 2013 MCIT announced that it would submit a Judicial Appeal to stop the ban issued by the Court, because of the impossibility of executing it.⁴¹ On 16 February 2013, the Association of Freedom of Thought and Expression (AFTE) submitted Judicial Appeal No. 10464 against the Court Order issued on 9 February 2013 by the Administrative Court and on 9 March 2013, the Egyptian Administrative Court halted the 9 February ban. The Court accepted an appeal by the National Telecommunications Regulatory Authority (NTRA) and AFTE, against the order.⁴²

39. France 24 Arabic at: <http://goo.gl/zh2uT> accessed on Wednesday 18 October 2012.

40. See Amenity press release YouTube ban in Egypt is a setback for freedom of expression <http://www.amnesty.org/en/news/youtube-ban-egypt-sends-dangerous-message-intolerance-2013-02-12>

41. See the MCIT press release http://www.mcit.gov.eg/Media_Center/Press_Room/Press_Releases/2561

42. See Ahram online <http://english.ahram.org.eg/NewsContentPrint/1/0/66452/Egypt/0/Egypt-court-halts-YouTube-ban.aspx>

CONCLUSION

Freedom of expression has a critical communications dimension. The Internet has become a major communications tool in Egypt - an aspect to be taken into consideration when drafting legislation. The protection of the freedom of expression and the right to knowledge are a joint responsibility to be observed by everyone, be them users, providers or the government.

Censorship policies are inadequate, and efforts deployed by the MCIT in developing e-governance structures under the ousted regime were important, but limited. Furthermore, multi-stakeholder policymaking processes are limited. This means that current legislative procedures do not provide an enabling environment which encourages innovative thinking, nor elaborate ways to develop service provider resources so that Internet development projects continue. State intervention must be limited to developing the infrastructure to enable broader use of the Internet.

Finally, differences of opinions are inevitable and an indicator which reflects freedom of opinion and expression. Political ideological shifts could pave the way for administrative intervention and over-regulation in Egypt. The Internet is part of this, even though it may have a negative impact on the Egyptian population.

IRAN

For several reasons, Iran has yet to fully utilise the Internet as a platform, mainly because of the ambiguous relationship between citizens and the establishment. Very severe prosecution and persecution are measures taken by the State in order to curb what it sees as a threat to the Iranian political system and the fabric of decent Islamic society. Nonetheless, Iran is also witnessing an excessive volume of online lawlessness⁴³ which can be attributed to a lack of Internet jurisdiction. It can also be argued that skewed attention to online activity in Iran has produced a vacuum which encourages harmful activities on the web. These conditions make Iranian Internet usage unique and some aspects of Internet governance less relevant, as outlined later in this report.

From a risk-analysis perspective, the Iranian establishment has a valid case for not promoting Internet access. Recent cases of cyber-espionage and sabotage in Iran provide a strong argument for limiting Internet penetration. Government plans to retract areas of public service which had been extended to the Internet back into physical offices areas, can be understood in this context. There is a prevalent assumption that the Internet is a vehicle for political and social change. However, it can be argued that the Iranian State's perspective on the Internet as a

framework for political instability and change is based on external attempts to use it in precisely that manner.

Many Iranians perceive the Internet as one of a limited number of means of engagement in political and social processes. Politicisation of the Internet narrows the perception of it to nothing more than a political entity. If it had not been regarded as hostile by the State, it could have been a more prevalent platform for other functionalities such as community development and social engagement.

Several factors including:

- (1) The unbalanced approach to Internet governance
- (2) Lack of interest in investing in and increasing Internet penetration rates, and
- (3) Politicisation of the Internet by major players including Western governments, outside NGOs and the Iranian diaspora, have resulted in a skewed Internet presence. Any serious discussion on current Internet presence in Iran and any realistic forecast for its future cannot and must not ignore these keys factors.

LAWS AND COMPUTER CRIMES

The regime's agenda dominates the Iranian legislative system. Vague and ambiguous laws can be used by the State apparatus to detain individuals, as and when it pleases. The 'Law of

43. Examples can be found, in Persian, on the website of Fata Police, the Iranian cyber police, at <http://www.cyberpolice.ir/> and Gerdab, which has stated ties with the IRGC, at <http://www.gerdab.ir/>.

Computer Crimes' which includes 56 Articles,⁴⁴ was approved by the Iranian Parliament in January 2009. This legislation has been instrumental in the prosecution and detention of several cyber-activists and bloggers.

A public prosecutor has categorised on his blog criminal content covered by this law as:⁴⁵

1. Immoral
2. Anti-Islamic
3. Anti-security and disturbing the public peace
4. Criminal regarding intellectual property and audio and visual issues
5. Content which encourages, invites or provokes others to commit criminal acts
6. Content which is against State and public institutions and their responsibilities
7. Content used to facilitate other computer crimes

Whilst content which encourages, invites or provokes others to commit crimes is illegal, so too is posting a link to this (potentially filtered) content on a blog or social network. With this in mind, the mere act of linking a source could be considered as criminal as actually promoting violence. The regime's lawmakers also consider content which encourages 'squandering' (being wasteful) as against the law. In a socio-theological context this includes any encouragement of consumerism so that anyone who uses the Internet for commercial or marketing purposes could be questioned. 'Squandering' has not been clearly defined, leaving room for interpretation.

44. <http://peyvandha.ir/0-2.htm>

45. <http://www.dadsetan.org/post-148.aspx>

Vague publishing laws also make it illegal to publish any content which speaks out against the State, contradicts the Iranian Constitution, or harms to the 'principles' of the Islamic Republic. Under this ambiguous law, what would be considered ordinary social media activity in other countries is potentially criminal in the Iranian context. In recent years this has resulted in many prosecutions. For example, the Iranian blogger Omid Reza Mir Sayafi⁴⁶ was jailed for insulting religious leaders, and died in prison in 2009. This case provoked a lot of local media coverage and became a benchmark in the history of the persecution of bloggers. This ambiguity makes it impossible for an activist to know when they have 'crossed the line' into illegal activity. This results in self-censorship, which also limits the use of the Internet for social and political activity.

In summary, the legal framework related to online activity could have severe repercussions for activists, and its ambiguity leads to limited participation through widespread self-censorship. This means that the Internet is not sufficiently cultivated for online social and political activism.

NATIONAL INTERNET: A "FILTERED" WORLD WIDE WEB

The Iranian regime aims to isolate its online citizens from the wider world, and its project to nationalise the Internet could assist them in achieving this goal. This Internet has been referred to by the Iranian authorities as 'Halal (clean) Internet'.

46. <http://globalvoicesonline.org/2009/03/19/omid-reza-mir-sayafi-iranian-blogger-dies-in-prison/>

The main goal of this project is to avoid the constant updating of filtering systems and new online technologies. As an alternative, the Iranian State means to create their own version of the Internet with limited content. This would allow citizens to roam freely on a 'national Internet', accessing information and interacting with business and official institutions. This would also give the Iranian regime full control of all data, including ways to deal with 'undesirable content'.

Reporters without Borders states that the concept of a national Internet is an attempt to combat the impact of the international Internet. The system '... consists of an Intranet designed ultimately to replace the international Internet and to discriminate between ordinary citizens and the 'elite' (banks, ministries and big companies), which will continue to have access to the international Internet.'⁴⁷ Others have argued that the Iranian regime's intention is to create an Internet where Iranians are 'safe' from pornographic content, hate speech and cultural influences which the World Wide Web permits, and that this project would still permit intra-national communications, commerce and business to prevail.⁴⁸

Ambiguity has also surrounded the 'national Internet' project since its inception, and has been linked to fears of disconnection and central control. In 2008 *Hamshari*, an Iran-based news website, wrote that 'national Internet'

is an ambiguous term.⁴⁹ In 2010 *Donayeh Eghtesad*, an Iran-based newspaper wrote that 'The project was an initiative of Ahmadinejad's government five years ago and it has still four years to go before it becomes operational... there is a curtain of ambiguity on this project. It is not clear what, where, how or who is going to use the national Internet ... The Minister of Communication and Technology, Reza Taghipour, says that the national Internet will be a broadband, fast network inside the country to answer the government's electronic needs ... At present, the Internet for households is provided by private companies, although the Ministry of Communication is researching the possibility of doing it by itself.'⁵⁰

Alireza Shirazi, the founder of a leading Iranian blogging platform, says that it has not been made clear to him what a 'clean Internet' is. However, he is concerned that, despite almost all social media being currently filtered, there will most likely be no Facebook, Twitter, Flickr, Myspace or any of the known social media services. He believes that instead of having an open Internet with a number of Internet sites on a filtered black-list, there should be a closed Internet with limited permitted sites.⁵¹

New Scientist magazine reported on the Halal Internet in its early stages. According to its security expert, Collin Anderson, the substitute network will contain Iran-specific content and alternatives for popular services including, for example, a substitute Facebook. The government

47. <http://en.rsf.org/iran-government-develops-national-03-08-2011,40738.html>

48. <http://www.aljazeera.com/indepth/opinion/2012/10/201210263735487349.html>

49. <http://www.hamshahri.org/news-62102.aspx>

50. http://www.donya-e-eqtesad.com/Default_view.asp?@=213707

51. <http://shirazi.blogfa.com/post-319.aspx>

would limit connections to outside networks, rendering them too slow to be unusable and thereby forcing users onto the national network.⁵² In October 2012, the Iranian media reported that 44,000 schools had been connected to the national Internet.⁵³ So far no information has been published regarding the characteristics of the interactions of these students and whether the network has become operational.

The National Internet Project (NIP) is a step backwards from the current filter-based framework. Some have argued that the tension around Iran's nuclear program, cyber-attacks and malwares targeting the Iranian nuclear facilities, have created an urgent need for the Islamic Republic to defend itself. The concept of a self-contained network has become a plausible and tempting alternative to the establishment. Nevertheless, given the enormous investment it demands in terms of infrastructure and security, it has been treated with scepticism. Although it is debatable, the latest cyber-attacks against Iran's nuclear program have been a contributing factor to the acceleration of plans for its implementation.⁵⁴

When President Mahmoud Ahmadinejad initially requested funding to launch the NIP in 2005, the Iranian Parliament refused the \$10 million funding.⁵⁵ That decision forced the government to seek other financing sources; however they

remain unclear. The NIP threatens the very trans-border concept which represents the basis of the Internet. Furthermore, the lack of information on its exact aims and its sources of funding leave serious doubts as to whether the Iranian regime will be able to launch such a massive undertaking.

FILTERING: AN EVERLASTING PROBLEM

The Iranian political regime has acquired and developed the technology to censor the Internet extensively. It can be argued that its filtering system is an extension of censorship practices exercised outside of Iran. As a result, different types of websites are being targeted with increasing regularity for censorship in a similar way to the physical world in which censorship is prevalent.

Abdolsamad Khoram Abadi, an official of the Iranian Judiciary, claimed that the Judiciary has blocked access to more than five million Internet websites perceived as immoral and anti-social.⁵⁶ In the official vocabulary of the Iranian state, 'immoral' does not only describe content of a pornographic nature. Civil society activists have also been labelled as advocating immorality. The Iranian filtering machine targets all kinds of websites, including news media and any which do not support the Iranian regime. This includes environmental blogs, social media websites, economic analysis websites and even unofficial pro-regime bloggers.⁵⁷

52. www.newscientist.com/article/mg21628865.700-first-evidence-for-irans-parallel-halal-internet.html

53. <http://khabarfarsi.com/ext/3595371>

54. http://www.washingtonpost.com/world/national-security/iran-preparing-internal-version-of-internet/2012/09/19/79458194-01c3-11e2-b260-32f4a8db9b7e_story.html

55. <http://www.hamshahri.org/news-131560.aspx>

56. <http://www.ettelaat.net/08-november/news.asp?id=33351>

57. <http://globalvoicesonline.org/2012/07/31/iran-pro-ahmadinejad-blogger-jailed/>

Filtering mechanisms were established during the introduction of the Internet to Iran. Strategies were developed in 2001, when the Supreme Council of the Cultural Revolution required Internet Services Providers (ISPs) to enforce filtering systems. A committee tasked with determining unauthorised websites was established and, as of 2009, private ISPs were required to pass their traffic through government-controlled channels.⁵⁸

The Iranian state does not advocate freedom of speech, and on 23 September 2012 the government announced that they would begin filtering Google and GoogleMail (gmail). A government official, Abdolsamad Khoramabadi, stated⁵⁹ that this was due to public demand caused by outrage at the presence of what was perceived as a blasphemous anti-Islamic video on YouTube (Google owns YouTube).⁶⁰ Khoramabadi is a key member of the Commission to Determine Instances of Criminal Content,⁶¹ a governmental body chaired by the Public Prosecutor which looks into controversial contexts and produces reports to the Head of the National Security Council. Its mandate is legally binding on all ISPs.⁶² However, this censorship did not last long, and gmail was unblocked. It was subsequently reported that the filtering system has adopted a new mechanism in order to block access to several audiovisual forms of content.⁶³

58. <http://iranprimer.usip.org/resource/new-political-tools>

59. <http://goo.gl/4ETN1>

60. <http://advocacy.globalvoicesonline.org/2012/09/17/did-google-do-the-right-thing/>

61. <http://internet.ir/law.html>

62. <http://globalvoicesonline.org/2010/11/23/iran-we-are-all-computer-criminals/> <http://globalvoicesonline.org/2012/09/24/iran-blocks-access-to-google-and-gmail-2/>

63. <http://advocacy.globalvoicesonline.org/2012/11/14/mena->

This more segregated filtering mechanism, whilst permitting access to a specific Uniform Resource Locator (URL), banned access to Internet protocols which provide audio and video content within that URL.

Given this, the safety of citizen content providers (such as bloggers) is indeterminate, as the thresholds of legality are not defined clearly. Whilst the regime resorts to censoring techniques, some technically savvy Iranians are able to access 'blocked' websites using circumvention services.⁶⁴

REPRESSION: VIRTUAL WRITERS, PHYSICAL VICTIMS

Iranian regime involvement in online affairs is not limited to activities in the virtual world. The regime has been known to detain bloggers and active users for voicing their opinions on social network websites. The legal ambiguity which surrounds web-users and online activists is not limited to individuals who oppose the state, but also pro-regime bloggers who have been prosecuted for their online activities. In July 2012 several pro-Ahmadinejad bloggers were arrested.⁶⁵ The regime does not discriminate between criticism in the online and physical world.

The Iranian State is currently working to become more effective and organized in their censorship process and in curbing activity on social media sites. In January 2011, the Iranian authorities

[netizen-report-porn-edition/](#)

64. <http://www.manoto1.com/ChannelNews/news1305>

65. <http://globalvoicesonline.org/2012/07/31/iran-pro-ahmadinejad-blogger-jailed/>

finalised the setting up of the Iranian 'Cyber Army', whose aim is to strengthen governmental control of the Internet. In May 2010, Ebrahim Jabari, an Islamic Revolutionary Guard Corps (IRGC) commander, officially confirmed the creation of an Iranian Cyber Army. The army had already been named in reference to several hacking and defacing efforts on the web. This acknowledgment confirmed the hacking of Twitter in December 2009 and Baidu (a Chinese search engine) in January 2010.⁶⁶

In April 2003, Sina Motalebi was the first Iranian blogger ever jailed on the grounds of blogging. He was arrested by the intelligence division of the law enforcement agency for publishing opinions on his personal blog and for interviews with foreign media. Sina's arrest was to set the tone for a long period of detention for Iranian bloggers. Between August and November 2004, Judiciary agents operating on behalf of Tehran's Chief Prosecutor, Saeed Mortazavi, detained more than 20 bloggers and online journalists. Several later provided accounts of ill-treatment while in custody.⁶⁷

On March 18 2009, Omid MirSayafi became the first blogger to die in prison under suspicious circumstances.⁶⁸ Omid was a journalist in the field of cultural affairs and ran a blog with a modest number of viewers. Nevertheless, he became a State target for allegedly insulting religious leaders in his personal blog. The latest victim is Sattar Beheshti, whose family was informed to prepare his body for burial after his

short detainment in prison in November 2012. He had been arrested for political activities on the social media website Facebook. Prior to his death, he told inmates and authorities that he had undergone severe torture whilst in custody. Accounts later published by his family, stated that his body exhibited clear signs of torture whilst in the custody of the State.⁶⁹

The 2009 disputed presidential elections were followed by new rounds of repression in the Iranian virtual world. Following protests against electoral fraud, the Internet took a leading role in organising and reporting on developments. This wave of online activity targeted everyone who was involved with brutality. As a result, several bloggers were given long prison sentences including Sakhi Rigi. He was arrested in 2009, accused of having published false information and for acting against national security; he was sentenced to 20 years in prison - the longest sentence ever passed for blogging in Iran.⁷⁰ In 2010, 18-year old Navid Mohebbi, active in the Iranian movement for women's rights, became the world's youngest imprisoned blogger.⁷¹

As social media has begun to take on a more prominent Internet role, the Iranian authorities have targeted them harshly - particularly Facebook. In January 2012, a group called 'Daaf and Paaf' ('hot persons') was seized by Iran's Cyber Army. The group held an online competition, the purpose of which was to select

66. <http://en.rsfi.org/internet-enemie-iran,39777.html>

67. <http://advocacy.globalvoicesonline.org/2008/12/19/iran-a-long-and-painful-story-of-jailed-bloggers/>

68. <http://www.march18.org>

69. <http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2012/11/opinion-dont-abandon-irans-internet-generation-to-online-oppression.html>

70. <http://advocacy.globalvoicesonline.org/2011/06/10/iran-record-breaking-20-year-jail-sentence-for-blogger/>

71. <http://en.rsfi.org/internet-enemie-iran,39777.html>

the most attractive male and female Iranian.⁷² Individuals from the police unit announced on the group's Facebook wall that 'the administrators of this group have confessed to have been promoting banality'. It was stated that posting pictures on Facebook of women without the veil, is punishable.⁷³

INTERNET CONTROL TECHNOLOGY

Research has indicated that commercial web-filtering products from the United States and Europe have been extensively used in Iran.⁷⁴ One such product is SmartFilter, now maintained by McAfee.⁷⁵ It has been suggested that Iran acquired these products through indirect means and that their use in Iran is a violation of the licensing terms.⁷⁶

Recent indicators suggest that Iran is no longer dependent on foreign filtering systems and is now using domestically manufactured filtering tools. A recent Freedom House report states that private ISPs are currently required to either use government-provisioned bandwidth or to send their traffic through filtering boxes provided by software companies based in Iran.⁷⁷

AmnAfzar Gostar-e Sharif (also known as Sharif SecureWare) - a software firm with filtering products on the market - was founded in 2002. The company states that it targets the security

requirements of enterprise and medium-level organisations.⁷⁸ AmnAfzar is located in Pardis Technology Park (PTP), a technology hub developed by the Technology Cooperation Office (TCO) of the Islamic Republic of the Iran Presidency. AmnAfzar manufactures the Unified Threat Management (UTM) system 'ParsGate' which is a firewall-designed to provide content-filtering functionalities and intrusion prevention.⁷⁹ 'Separ', an Iranian web-filtering product also provided by Amnafzar, is another product which provides URL-filtering functionalities.⁸⁰

Filtering of the Internet is commonly assessed for its social and political implications. However, these are essentially technological endeavours and demand either the import of necessary equipment or self-sustained set-up. Whilst the Iranian Internet Censorship system was initially based on technology and tools adopted from Western providers, it has now moved toward a domestically-erected and maintained industry. This limits the possibility of weakening it through sanctions and embargoes.

ACCESS TO INFORMATION

A 2011 report published by the Foreign Policy Centre⁸¹ reviewed the current situation of access to information in Iran from a human rights perspective.⁸² Sections of this report were written by Iranian social and political activists

72. <http://globalvoicesonline.org/2012/01/30/iran-police-controls-facebook-group-arrests-its-administrators/>

73. <http://ilna.ir/news/news.cfm?id=16099>

74. <http://opennet.net/studies/iran>

75. <http://www.mcafee.com/ca/products/smartfilter.aspx>

76. <http://www.newscientist.com/article/dn7589-iranian-net-censorship-powered-by-us-technology.html>

77. <http://www.freedomhouse.org/report/freedom-net/2012/iran>

78. http://www.amnafzar.com/aboutus_eng.html

79. http://www.amnafzar.com/Pg_eng_0.html

80. http://www.amnafzar.com/Separ_eng_0.html and http://web.archive.org/web/20111005032131/http://www.amnafzar.com/Separ_eng_0.html

81. <http://fpc.org.uk/>

82. <http://fpc.org.uk/fsblob/1369.pdf>

based outside the country. The report describes many narratives regarding the blocking of Internet access during current socio-political developments in Iran, as well as efforts by the activist community to provide training and alternative access mechanisms.

The report interviewed Saeed Valadbaygi, an activist in his late-30s based in Toronto, Canada. Saeed describes the challenges caused by the low speed of available Internet connections in Iran, hurdles caused by the pervasive filtering system and frequent attempts by hackers backed by the Cyber Army to infiltrate and shut down dissident sources. Saeed describes methods used by him and other activists outside Iran to provide alternative connections, including rerouting Internet traffic. As stated in the above report, 'To upload five minutes of footage on YouTube could take 50 minutes at home, so we use proxies through alternative domains, so the person in Iran is in effect uploading the video via our computers outside the country.'

It is clear that access to information via the Internet in Iran has been following a downward spiral. A 2011 study commissioned by Nokia Siemens Networks investigates the Connectivity Score of different countries.⁸³ This study assesses how 'usefully connected' various countries are - defined to 'encompass usage and skills as well as infrastructure'.⁸⁴ The report assigns a score of 2.41 to Iran - just below the median score of 2.73 for the group of Resource and Efficiency-driven Countries.⁸⁵ The report

suggests that Iran shows strong growth potential and yet is one of the least developed Information and Communications Technology (ICT) markets in the Middle East. It concludes that Iran's telecommunications market is challenged with excessive regulations and legal hurdles. The government of Iran is described as exerting a lot of control over the market and being the owner of most telecommunications companies.

Iran was one of the first countries to adopt the Internet in its early stages. An early report entitled *The use of the Internet in Iran* was published in 2002 in the Journal of Educational Technology Research and Development.⁸⁶ It tracks the first wave of Internet interaction through the Institute of Studies in Theoretical Physics and Mathematics (ISTPM). Figures from 1996 estimate the number of Internet users at more than 60,000. This number is based on account holders in the Institute for Research in Fundamental Sciences (IRFS). The report concludes with an optimistic forecast for the growth of Internet access in Iran. However, it has not been able to follow other countries in its class, by extending usage.

Content published and consumed on the Iranian Internet has a strong socio-political element and is generally not in favour of the Iranian establishment. Consequently, access to Internet information has strongly positively correlated with criticism of and opposition to the Iranian establishment and has led to a defensive attitude towards the Internet by the establishment. Internet access has become

83. <http://www.connectivityscorecard.org>

84. <http://www.connectivityscorecard.org/faq/>

85. <http://www.connectivityscorecard.org/countries/iran>

86. Johari, Abbas. "Internet Use in Iran: Access, Social, and Educational Issues." *Educational Technology Research and Development* 50.1 (2002): 81-84.

a victim of efforts by the Iranian establishment to control social interaction and public debate in Iran. It has been argued that the Iranian Internet prematurely adopted a strong political identity which resulted in the State acting against it.⁸⁷

E-GOVERNMENT

E-governance is the effective use of information technologies to facilitate public administration. It necessitates the adoption of new skills and processes by government organisations and citizens. Therefore, strong incentives are necessary for both government and citizens to proceed through this modification of the public sphere.

An academic thesis, published by Lulea University of Technology in Sweden, examined the role of the Ministry of Commerce in establishing e-governance in Iran.⁸⁸ The thesis investigated several e-government readiness models available in the literature and suggested a novel one. A questionnaire was given to managers and staff at the Ministry of Commerce, and a list of obstacles was derived from statistical analysis of the responses on the questionnaire. They were as follows;

- IT Infrastructure obstacles.
- Social and cultural obstacles
- Lack of IT skills
- Legal and security-related obstacles

A similar assessment was carried out in a 2002 study on the e-government maturity status of 25

government agencies.⁸⁹ The authors of the report examined their online facilities and ranked them according to UN e-government benchmarks of 'maturity'.⁹⁰ Results indicated that the highest rank was assigned to the Atomic Energy Organization (ranked at 'enhanced'), whilst six organisations were ranked as 'non-existent' and the rest as 'emerging'. The relatively slow rate of adoption of e-government concepts in Iran is combined with a decline in the current position of the country when measured against internationally-devised and accepted scales of e-government utilization.

The National Cartographic Centre of Iran (NCCI) is the main authority for producing spatial information, and acts under the President's Deputy for Planning and Strategic Supervision.⁹¹ Two directors of the NCCI have recently provided an analysis of the role of the NCCI in the development of e-governance.⁹² The paper cites results from United Nations reports on e-government,⁹³ which indicate that between 2005 and 2008 Iran has increased its e-government readiness. The same report, however, puts Iran in the 98th and the 108th

87. A more complete profile of Internet access in Iran is available on the Open Net website <http://opennet.net/research/profiles/iran>

88. <http://epubl.ltu.se/1653-0187/2007/052/>

89. Ghasemzadeh, Fereidoun, and Safari, Hossein. "E-Government Maturity Level: A Study about Iran." *EurAsia-ICT. Proc. of EurAsia-ICT 2002*, Shiraz, Iran. Pages 231-35.

90. "Benchmarking E-Government: A Global Perspective-- Assessing the UN Member Status", United Nations - Division for Public Economics and Public administration, May 2000.

91. <http://www.ncc.org.ir/HomePage.aspx?TabID=1&Site=NccPortal&Lang=en-US>

92. Sarpoulaki, M., A. Eslami Rad, and A. Salekniac. "E-Government Concept and Spatial Information: A Case Study in Islamic Republic of Iran." *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*. Beijing. Vol. XXXVII. Part B4, 2008. 19-24.

93. <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan028607.pdf>

out of 192 ranks in the years 2005 and 2008, respectively. The authors conclude that this indicates how much slower Iran's approach towards e-government has been in comparison to the world average.

Similar results are reported in a 2010 report published by the Statistical Economic and Social Research and Training Centre for Islamic Countries (SESRTC).⁹⁴ The report examines the status of members of the Organisation of Islamic Cooperation (OIC) in terms of e-government development and e-participation.⁹⁵ According to this report, in both 2007 and 2009, Iran had one of the lowest ranks in the group.

While such studies independently indicate that the growth of e-governance in Iran is slower than many other countries in its category, an assessment of the political conditions in the country also shows a lack of willingness to invest in and rely on moving government services over to the Internet. Recent cyber-attacks on several key ministries, including the sensitive Ministry of Petroleum, have convinced the establishment that a counter-move is necessary and, as a result, key ministries are to go offline. This was indicated by the Minister for Telecommunication Minister in an August 2012 interview.⁹⁶

The move towards further adoption of e-government concepts and institutions is in direct conflict with the centralized security-minded authority presently existing in Iran. As elements of democratisation lose their

effectiveness, a move toward more open and responsive governance will clearly not be a priority. Consequently, a detailed investigation of current transparency and accountability of e-government in Iran is challenging.

The reasons why Iran should be pushing for more e-government services are presented in various publications. For example, a 2011 paper⁹⁷ examined the level of satisfaction amongst Iranian citizens regarding the Electronic Value Added Tax (EVAT) system implemented by the State Tax Organization (STO).⁹⁸ Researchers used a web survey method and concluded that efficiency, completeness, and usability were found to be the most significant contributors to overall satisfaction, while customization, reliability, and accessibility had a lower impact on overall satisfaction.

THE IMPACT OF SOCIAL MEDIA ON CIVIL LIBERTIES

Western mainstream media has generally praised the Internet, and social networks such as Twitter and Facebook, are becoming increasingly significant influences on Iran's socio-political situation. The 2009 presidential election was famously called the 'Twitter Revolution'.⁹⁹

During times of crisis, social networks have carried timely information regarding developments

94. <http://www.sesric.org/sesric-about.php>

95. <http://www.sesric.org/files/article/407.pdf>

96. <http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9453905/Iranian-state-goes-offline-to-dodge-cyber-attacks.html>

97. Yahya Sheibani, M., & Fariborzi, E. (2011). E-Government services in Iran: Looking at citizen satisfaction. 2011 International Conference on Communication Engineering and Networks (ICCSIT), 19, pp. 19-24. Singapore: IACSIT Press.

98. http://www.vat.ir/ConceptVAT_htm.htm

99. <http://www.washingtontimes.com/news/2009/jun/16/irans-twitter-revolution/>

in Iran. Nevertheless, the idealisation of Internet-based tools as vehicles of progressive change has been criticised. Evgeny Morozov comprehensively assesses the functions of the Internet in less-democratic countries in his book *The Net Delusion*.¹⁰⁰ Morozov focuses on Iran to discuss cyber-utopianism - the assumption that the Internet is an all-good tool, which can radically transform societies into better conditions without side-effects - and cyber-centric approaches - the recommendation to activists in the field to focus their efforts on cyberspace. He compiles evidence to show that cyberspace can be used equally by different sides of a political struggle. He argues that the proponents of a closed society can benefit from online platforms as much as those seeking more liberal values do. On the other hand, Morozov discusses the implications of an unbalanced approach when it comes to performing social and political campaigning on the web. He argues that the nature and potential outcomes of offline and online advocacy attempts are intrinsically different.

A recent report by the Iran Media Program (IMP) examines the ways in which Iranians access news and information.¹⁰¹ The report suggests that assertions on the role Twitter played in the Iranian uprising could have been over-stated. The report also shows that the State-run TV and domestic press remain the two most prominent sources for news in Iran, with the Internet occupying sixth place after Radio.

Another Iran Media Program report discusses

the relief effort - which used the Internet as a catalyst for online coordination - for victims of the 2012 earthquake in Azerbaijan.¹⁰² The report provides a short commentary on the impact of social media in times of crisis, including criticism of weak coverage by the State-run broadcasting body Islamic Republic of Iran Broadcasting (IRIB). It compares the online mobilisation which occurred after the earthquake, with the aftermath of the contested 2009 presidential elections in Iran. This earthquake is rated as one of the three main causes which united online Iranians (the other two being the campaign to replace 'Arabian Gulf' and 'Persian Gulf', and efforts to support Iranian athletes on the international scene. The author suggests that 'IRIB's apology and Khamenei's visit to the quake-hit areas' are consequences of online efforts.

Assessment of the nature and extent of interactions between the Iranian users of different social networks indeed indicates that these platforms have given the population a new means for social and, to a lesser extent, political involvement. However, their role in influencing developments on the ground, has been over-estimated. Such over-statement is not only theoretical, but has had wider practical drawbacks. For example, the assertion that Facebook and Twitter have the ability to, or have succeeded in playing, a political role beyond the reality, has exaggerated their influence. However, this mistaken understanding has both radicalised the environment and agitated the establishment to take up an offensive position. As a result, it is argued that these social networks have not been able to accept a more neutral, and

100. Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs, December 2010

101. <http://www.iranmediaresearch.org/en/research/pdf/990>

102. <http://www.iranmediaresearch.org/en/research/pdf/1055>

therefore more effective position. The hyped-up labelling of social media platforms as political game-changers has actually limited their political efficiency.

There is no doubt that online social networks have become part of the fabric of society in many parts of the Iranian population. However, many are sceptical of the nature and extent of their accomplishments in social and political change.

CONCLUSION

Analysis of the role of the Internet in Iran, and the assessment of its current (and projected) position in Iranian society must include careful attention to the relationship between the Iranian establishment and its citizens. For example, the clear presence of an active legal framework on the Internet is generally perceived as upholding the values and identity of Iran's ruling class. This framework allocates minimal resources to maintaining order on the web, unless it is felt that issues such as modesty and national security are at stake. Filtering is the key component of Internet policy in Iran. Nevertheless, many in Iran have found successful circumvention through the filtering system.

While Internet-filtering endeavours in Iran began with the consumption of foreign technologies, many major parts of the Iranian filtering system are now manufactured domestically. Nevertheless, the system is dissatisfied with the performance of the current filtering framework, and the possibility of establishing a domestic alternative to the International World Wide Web is now under discussion.

Many argue that the NIP is too difficult an undertaking for the Iranian regime. Repeated delays and the many conflicting narratives of what it will be able to accomplish, are cited by some observers as evidence for the nationalisation of the Iranian Internet facing major, perhaps insurmountable difficulties.

Due to legal ambiguity, harsh treatment of online activists in Iran has become a reality for many bloggers, online journalists, and even ordinary users of social networks. Cases of mistreatment, long prison sentences, and even death in custody, have been documented in relation to Iranian online activists. In this hostile environment, and as the Internet becomes a battleground between the establishment and its opponents, processes such as e-government are the victims.

Hostility on the net is not limited to confrontations between the Iranian regime and its citizens. Sensitive parts of the Iranian political and economic machinery have been targets of international espionage and sabotage attempts. Compared to other countries, Iran has been slow in adopting online governmental concepts. Because of this the regime tends to pull back its essential services from the web and citizens lose out.

Many sectors of the Iranian public have used the Internet to engage with the regime. However, this has proven to be less true of the physical world. It is therefore an over-simplification to suggest that the Internet is the main enabler of democracy in Iran.

The role of the Internet is extremely complicated and cannot be assessed in a reductionistic fashion. Whilst providing social and political

engagement, it has also been over-politicized and subsequently has failed to perform when it comes to liberalising the political platform.

RECOMMENDATIONS

In many respects the virtual world mirrors the physical one, and the regime aims to control many aspects of both public and private life. The Internet, however, provides ways for average citizens to escape the cultural hegemony of Iran. People can express themselves and come together online for diverse reasons which include supporting campaigns, exchanging ideas, and content searching.

It is not only the politically-charged activities of Internet use which disturbs the Iranian state, but its mere existence as a space for sharing. The State continues its path to curb social capital on the Internet and shows no signs of change. Nevertheless, three initiatives could make it safer and easier for both users and the State.

1) A CALL TO POLICY MAKERS IN IRAN

Iranians used social media tools effectively in helping victims of the 2012 earthquake.¹⁰³ Many donated their blood; others sent goods. Both domestic and foreign media should focus on this non-political use of the Internet to emphasise the positive role it can play in Iranian society. This could modify the hostile image of the Internet held by some Iranian policy makers. Policy makers could begin to accept the Internet as

a social, rather than merely a political, enabler and could avoid underpinning the current international perspective with continued uncertainty. For example, on 13 August 2012, the ultra-conservative newspaper *Keyhan* wrote 'The event [earthquake] has provided the dishevelled opposition groups a good excuse to reorganize and re-energize themselves.'

However, the Islamic Republic is composed of different factions, some of whom express contradictory opinions from time to time. This dynamic enables those within the regime to use this disagreement to modify the image of the Internet to suit the regime. Ultimately, when an earthquake hits, it does not differentiate between victims, whether pro-regime or pro-democracy.

2) A CALL TO THE WEST

Due to International sanctions, two of the best-known free antivirus programs - AVG and Avast - last year prevented Iranian Internet Protocol users from downloading their software or updating their virus definitions. Whilst this has not been mandated by a sanction, it is the fact of the ground. Similarly, Adobe does not permit Iranian users to download its free Flash and PDF-reading software. These tools are used by hundreds of millions of people across the globe. This is particularly important in the case of Adobe Flash Player, the dominant streaming video plug-in. Western global corporations must provide the technology needed by the Iranians to secure their computer networks.

103. <http://www.arsehsevom.net/2012/08/eager-to-help-iranians-respond-to-earthquakes/>

3) WAKE-UP CALL FOR IRANIANS

Iranian cyber-activists have been increasing their use of Western sites such as Facebook, YouTube, WordPress and other blogging tools, and have created their own platforms such as Balatarin.¹⁰⁴ This is reminiscent of Digg, and Gooya,¹⁰⁵ which served as a political ‘yellow pages’ before blogging, and predated blogging when they expanded into news-gathering and political forums.

The turmoil of 2009 attracted the attention of the world, and the Iranian online community proved capable of becoming an important part of the Iranian journey towards democracy. The question is what this diverse and talented community has been able to accomplish in terms of innovation, or even imitation of ideas which are already available on the Internet.

104. <http://balatarin.com/>

105. <http://gooya.com/>

IRAQ

With its ability to connect billions of people globally in order to exchange information quickly and effectively, the Internet is widely considered to be the 20th century's biggest invention. It is a fast-growing platform with diverse and evolving applications and services and has become a staple of many people's lives. However, governments in the Arab region may not welcome it because of local political conditions, seeing it as a non-compliant and uncontrollable environment. With its freedom of expression and dialogue on human rights and democratic principles, it may not fit the mindset of rulers in the area.

Such governments attempt to regulate the Internet through legislation, thus limiting local content and usage in the name of protecting higher national interests. To counteract such restrictions, a global campaign about Internet Openness has arisen. Accessibility, freedom of expression, resourcing, security and privacy are all comprehensively discussed at both local and regional levels with international and regional organizations striving to increase awareness. Internet Openness is a multi-disciplinary theme.

The national Constitutions of advanced countries such as Finland consider an open Internet to be a basic human right. By this definition, censorship in the Arab region has resulted in continuous violation of this right. During events of the "Arab Spring", the first action taken by the Egyptian government was to shut down

the Internet. This inhibited the aspirations and demands of citizens and suppressed the virtual connections and coordination of protestors. However despite such desperate governmental measures, successful revolutions continued.

EXECUTIVE SUMMARY

This report will examine the status of Internet openness in Iraq in terms of:

- Internet history and background in Iraq
- The current situation - Internet openness and content filtering
- Internet legislation, policy, regulatory environments and frameworks
- Challenges, barriers and limitations to Internet openness
- Access to Information status and e-participation
- Transparency and accountability
- Local civil society conditions and the impact of social media on civil liberties
- Stakeholders – who they are and what they do
- Social networks, where bloggers, journalists, activists and human rights defenders are actively involved in Internet freedom, policy processes, privacy and secure online communication.

The report will conclude with a list of recommendations to influence policy-makers

and government executives and address Internet openness in the future.

INTERNET BACKGROUND IN IRAQ

Over the past three decades, Iraq has suffered a cumulative deterioration due to three major wars, international trade sanctions and political instability. Prior to the 2003 US-led invasion, the Internet, along with other modern technologies such as mobile phones and satellite, were prohibited by the strict control of the Islamist regime. Iraq was the *only* country in West Asia with no Internet connection. Since the invasion, modern technologies, including the Internet, have been launched, making Iraq relatively new to the Internet age. Services are provided mainly via Asynchronous Digital Subscriber Line (ADSL) by the State Company for Internet Services (SCIS) - a company owned by the Ministry of Communications (MoC)¹⁰⁶ - and a few local ISPs using wireless technology.

However, recent political changes are not reflected in Iraqi Internet penetration. The latest statistics show it remains the lowest and poorest in the Middle East despite more than eight years of change. Figures from the end of 2011 show:

- Internet users rate = 5.6%¹⁰⁷
- 'Households with Internet access at home' rate = 7.5%¹⁰⁸
- Fixed-telephone subscriptions rate = 6.0%¹⁰⁹

- Internet penetration rate = 4.3%¹¹⁰

These figures are due, in no order of importance, to the following reasons:

- Poor inherited telecommunications infrastructure based on copper connections.
- Absence of a high-speed network to connect both nationally and internationally.
- No plan for public broadband Internet deployment. (A very small broadband connection is available only to elite Government of Iraq (GoI) officials.)
- Lack of a unified national telecommunications law and regulatory framework.
- Vague telecom regulations. Regulatory decisions are made by the MoC.
- An outdated business model of a single, state-owned, nationwide ISP operator – SCIS.
- General continuous nationwide instability - sectarian tensions and terrorism.
- Very poor national electrical supply and services. Current Iraqi electricity demand is estimated at 27-30 Megawatt (MW), whereas capacity is only 6-8 MW. This shortage is substituted by home diesel generators, afforded only by the rich.
- The deliberate disablement, under the pretext of fears of espionage, of the optical fibre project which connects countries bordering Iraq with the outside world.
- State corruption; Iraq is ranked 175 / 183¹¹¹ on a global Political Corruption Index.
- Lack of a national governmental Information and Communications Technologies (ICT)

106. www.moc.gov.iq

107. <http://www.itu.int/ITU-D/ICTEYE/Default.aspx>

108. http://www.itu.int/ITU-D/ict/publications/material/LDB_ICT_2012.pdf

109. *ibid*

110. <http://www.internetworldstats.com/stats5.htm>

111. <http://www.transparency.org/country#IRQ>

policy and related capacity-building programs.

- Unsurpassed deployment of a vaguely-specified e-government project.
- High national poverty rates (25%-40%) and high rates of internally-displaced people due to sectarian violence and fear.
- Intermittent international community aid and representation.
- A huge lack of Human Resource (HR) skills due to the emigration of Iraqi intellectuals.
- Political issues including continuous local political conflicts, biased political parties and appointment of ministers, lack of ministerial vision and volatile successive sectarian GoI executives leading to poor achievements and corruption.

CURRENT SITUATION OF INTERNET OPENNESS IN IRAQ

The overthrow of the regime in 2003 was a milestone in the emergence of complete Internet openness in Iraq. Since then, chaos ensuing from the absence of a State has provided a free atmosphere for Internet availability via quickly-deployed and widespread Very Small Aperture Terminals (VSAT). The new Iraqi Constitution of 2006¹¹² protects freedom of expression so long as it does not violate public order and morality.

Accordingly, from the official government side, Internet access and openness in Iraq remains largely unaffected, i.e. GoI have not made any steps to measure Internet control. The current clear image is that the media scene has changed

completely and a booming number of media activists are using the Internet to express their opinion, criticize all GoI aspects, and share ideas openly and freely without censorship. Although some journalists and activists have been killed by insurgents and coalition forces, their deaths were mainly due to the usual clashes which can occur in any hot-fields coverage, i.e. their killings were not due to their individual Internet activism, as reported by many independent observers. Furthermore, Iraq does not have an official national Internet-filtering policy and there is no evidence that the State ISP (SCIS) practices filtering. Open Net Initiative (ONI),¹¹³ an international Canadian agency working in Internet censorship, conducted a 3-year test (2007-2009) of in-country tests on two Iraqi ISPs - SCIS (the State-owned principle ISP which controls most Internet traffic) and a selected private sector ISP Itisaluna. Results revealed no evidence of technical filtering for any category tested.

The GoI has recently declared plans to block “immoral” (read ‘insurgent’ and ‘terrorist’ groups) web content and has ordered the licensing of public Internet cafés by an independent regulator – the Communications and Media Commission (CMC)¹¹⁴. In February 2009, the MoC stated that it would implement a security system to monitor the Internet and block access to online content where there is concern over national security. However, neither of these steps appear to have been activated since all Internet websites, including the popular social ones - Facebook, YouTube, Twitter - remain accessible.

112. www.uniraq.org/documents/iraqi_constitution.pdf, www.cabinet.iq/dostor.htm

113. <http://opennet.net/research/profiles/iraq>

114. www.cmc.iq

General freedom of speech, and particularly on the Internet, is a positive indicator of the new Iraq where activists, bloggers and observers heavily criticize Gol and ICoR performance with no restrictions. To date there have been no solid claims of violations of freedom of expression by the Gol. The only violations of human rights have been where armed insurgents in Iraqi jails claim to have been badly treated.

ACCESS TO INFORMATION STATUS IN IRAQ AND E-PARTICIPATION

The Gol has adopted Constitutional policies regarding non-censorship and freedom of expression.¹¹⁵ Diverse civil society organizations, including those working in human rights and the media, have been able to work freely online. Iraqi Ministries have also started to form policies around building their own websites and creating online content. However, there is still a long way to go before information access and e-participation will be achieved.

Online information access and e-participation for citizens is poor for a number of reasons, including poor Internet access penetration rates, a lack of ICT education following three decades of international isolation, very poor electricity availability, mistrust of the Gol and general factors relating to hardship. The Gol e-Gov project has no specific portal and the project, started in early May 2003, is still only on Gol intra-connections. It has not gone public and with the current political conflicts and poor administration, the Gol have no intention of establishing standards of open government data.

115. www.uniraq.org/documents/iraqi_constitution.pdf, www.cabinet.iq/dostor.htm

To overcome this negative image, infrastructure modernization and a huge ICT-awareness and training program is needed. The Gol will not be able to act alone, and international aid and real Public-Private Partnership (PPP) schemes will be required. A solid building program and trusting relationships between the State and citizens are also necessary. The Iraqi people are waiting eagerly for such measures.

For most Iraqis, primary daily concerns are for safety and security. Distrust of the political scene, together with general fear and uncertainty make online access and e-participation a low personal priority. Citizens are also not sufficiently informed to suggest fruitful Internet policies which will engage them.

IRAQI INTERNET LEGISLATION, POLICY, REGULATORY ENVIRONMENTS AND FRAMEWORKS

The Communications and Media Commission (CMC)¹¹⁶ was established in 2004 to act as an independent and exclusive regulator of the media and telecommunications in Iraq. This sets a new historical precedent. It has imposed a Code of Ethics on the media where content relates to security and sectarian tension. Despite this, both media channels and individuals are free to post on freely-accessible social sites such as Facebook. Furthermore, CMC has not imposed ISPO regulation, thus meaning that the Internet is completely open and there have been no claims or witnessed arrests of bloggers or journalists as a result of online activities.

116. <http://www.cmc.iq/en>

There is a general policy vacuum with regard to the Internet and ICT. Such policies would need to be drafted by the MoC, then discussed and approved by the Iraqi Council of Representatives (ICoR).¹¹⁷ In 2008 the MoC, with the help of the World Bank (WB) drafted three new laws: *Telecomm. Liberalization and free market, MoC Privatization, and CMC regulation*. Five years later, these laws, aimed at restructuring the national Telecom sector, are still under discussion. The delay in ICoR corridors is due in part to the way in which politics functions generally in Iraq. However, ignorance is also a factor. Conflict between ICoR and the Gol generates poor collaboration and mistrust.

The Gol was in the process of enacting an *Iraqi Information Crimes* law to regulate the use of information networks, computers and other electronic devices. The law had its first reading on 27 July, 2012. The proposed legislation was analysed by many international organizations, including Human Rights Watch (HRW)¹¹⁸ and Article 19,¹¹⁹ both of whom found that it violates the international standards for freedom of speech. At local level, Iraqi activists launched a Facebook campaign¹²⁰ to oppose the draft. Their major concerns related to the vagueness of its provisions, the severity of punishments for violations, and that the Gol could use it to punish political criticism. On 6 February 2013 the Iraqi parliament revoked and cancelled the draft law due to the scale of both local and

international objections.

IRAQI CHALLENGES, BARRIERS AND LIMITATIONS

Despite the post-2003 promised transformation of Iraq from a centralised State to a modern free market, very little has been done in the telecommunications and Internet sectors. The following, in no particular order, are clear negative indicators:

1. There is no real ISP competition: There is one state-owned ISP (SCIS) with legacy copper networks, which does not cover the whole country.
2. There is a vacuum in legislation and policy. Several telecommunications and privatization laws have been drafted since 2008, although none have been discussed in the ICoR. The MoC has no nationwide Internet or IT development policy.
3. CMC, the only constitutional independent regulator, collaborates poorly with the MoC. CMC and MoC roles overlap and intersect when, according to international professional standards, their work should be separated. Flaws and violations of this relationship include:

(1) On the one hand, CMC is too closely related to ICoR administration. CMC leadership should be appointed via a competitive and transparent process. However, currently, and for many years now, CMC leadership has been appointed by the Prime Minister's Office (PMO) thus meaning that the PMO effectively controls the ICoR.

117. <http://www.parliament.iq/english/>

118. <http://www.hrw.org/reports/2012/07/11/iraq-s-information-crimes-law>

119. <http://www.article19.org/resources.php/resource/2792/en/Iraq:%20Draft%20Informatics%20Crimes%20Law>

120. <https://www.facebook.com/No4ICLinIraq>

CMC is therefore not independent, but represents GoI interests.

(2) On the other hand, MoC (represented by SCIS), should be a competitive operator, amongst other private operators regulated by CMC rules. However, SCIS is currently the only major operator, whilst also regulating its own work.

4. In an effort to promote foreign investment and rebuild the country, the GoI established the National Investment Commission (NIC)¹²¹ in 2006. NIC law was passed by the ICoR in 2008. Having identified the poor quality and slow speed of communications infrastructure as its largest obstacle, the NIC included the Iraqi telecommunications and Internet sector in its investment interests. It classified five nation-wide projects with regard to fibre optics backbone, connectivity, public switch networks, landlines and telecom connectivity with neighbouring countries.¹²² The NIC has not attracted any investment so far, mainly due to the obstacles of heavy bureaucracy, very tough Iraqi VISA restrictions and security clearance procedures, poor national security, the high GoI corruption index, a poor and outdated banking system, and very poor basic electricity and water services.
5. From 2003 the Iraqi e-government project,¹²³ funded by the Italian Government, has been one of the early promising projects. However,

since then administration of this project has been moved between many GoI entities and there has been little public access.

6. The assassinations of Iraqi academics and qualified intellectuals¹²⁴ have had a destructive effect on general national development. Many survivors, intellectuals and technocrats have emigrated. In 2008, the Iraqi government issued a stimulus package aimed at prompting them to return. However, most have not done so, due to concerns about security and disbelief in GoI promises to appoint qualified technocrats rather than sectarian executives.
7. Electricity supply is the most urgently needed service in Iraq. Since average national grid supply to homes is 4 hours per day and diesel generators can only be afforded by the rich people, Internet service and access rates are very low.
8. Political instability has a major negative impact on all aspects of Iraqi life. For example, the Minister of Communications, a member of the second largest national political party, was obliged to withdraw from his post three times, following his party's withdrawal from ICoR and the GoI. Since no other Minister is permitted to fulfil his role in his absence, the cumulative 2.5 years of absence has left a vacuum in MoC operations. During the writing of this report the Minister officially resigned,¹²⁵ protesting against a long list of intractable and accumulated barriers including political intervention in the work of

121. <http://www.investpromo.gov.iq/index.php?id=1>

122. www.investpromo.gov.iq/tl_files/NIC%20Sectors%20Provinces%20and%20Projects%20jan%202012_v3.pdf

123. <http://www.infoworld.com/t/platforms/italy-iraq-agree-strengthen-e-govt-cooperation-348>

124. <http://www.brusseltribunal.org/academicsList.htm>

125. <http://ipairaq.com/?p=437>

the MoC, suspicious contracts (serving top Gol executives' interests), the imposition of the Gol on MoC ministerial power, the collapse of MoC corruption investigations by the PMO and the disabling of strategic MoC projects by powerful politicians. The PMO accepted the Minister's resignation immediately without investigating the issues raised. However, it creates a new vacuum for MoC operation and it is unlikely that further progress will be made.

CONCLUSIONS

- Internet access and openness in Iraq is largely unfettered. There is currently no evidence of content filtering. Civil society activists freely express their opinions via local websites and on international social networks such as Facebook and Twitter.
- Even when compared with countries in the region, Iraq is badly lacking in ICT, Internet penetration and information measures. It is not included in international figures such as The World Economic Forum (WEF), *GITR Global Information Technology Report 2012*,¹²⁶ the *AWCR Arab World Competitiveness Report 2011-2012*,¹²⁷ or the International Telecommunications Union (ITU) report on *Measuring the Information Society-The ICT Development Index 2011*.¹²⁸
- Iraqi online information access, accountability, transparency and e-participation are very poor due to poor infrastructure, policy and legislative processes.¹²⁹
- The major obstacle to Internet development (both legislation and projects) is the political situation where ICoR and Gol bodies are conflicted, mistrusting, inefficient, hostile, and lacking in professional vision. This is compounded by both media and armed attacks against each other, thus decreasing internal security. The ICoR and Gol are corrupt, incompetent and ignorant of requirements.
- Since Iraq has one of the highest corruption indexes in the world, vaguely-interpreted and implemented laws, no on-the-ground measures, procedures or statistics and incompetent Gol executives, it is very difficult, if not impossible, to speak about Iraqi transparency and accountability.
- A draft version of the *Iraqi Information Crimes Law* is currently being debated. There are fears that this law, if approved, could form part of a future broader pattern of restrictions on general freedom of expression, and that the Gol may use it to initiate measures to censor Internet content and monitor online activity.

126. http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

127. http://www3.weforum.org/docs/WEF_AWC_Report_2011-12.pdf

128. <http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5>.

pdf

129. <http://www.giswatch.org/es/node/31>

RECOMMENDATIONS FOR THE WAY FORWARD

- For overall national stability and long-awaited development, there is an urgent need for post-conflict reconciliation strategies and political reform. This is a necessary foundation for sustainable works by the MoC and CMC.
- A radical solution is needed for the provision of basic services including electricity.
- The GoI generally and the MoC specifically, must recognize that the very poor statistics for Internet and telecommunications service provision are shameful, given that Iraq is the world's second richest oil-State. The GoI and MoC must understand that Internet access is vital for positive socio-economic transformation, and push projects to modernize. This could include nationwide projects and timely plans for Optical Fibre Networks and Connectivity, Broadband and Fibre To The Home (FTTH) as well as e-government project implementation.
- The GoI must revive and boost the existing e-Gov project to gain the promised better online information access and e-participation for its citizens. The GoI must set policies to disclose its data to the public in order to enhance transparency and accountability and to regain the trust of citizens.
- The CMC must demystify and create clear visions and work procedures for a truly independent regulator, including openness to more ISPs to provide competition.
- The MoC must form and adopt updated and implementable Internet and ICT policies with private sector investment. This may include infrastructure sharing.
- The ICoR must speed up the long-awaited MoC legislation on *Liberation and Privatization of the Telecommunications Sector*. It must reject the proposed drafted *Iraqi Information Crimes Law* and engage in comprehensive reforms to Iraq's legal framework in order to guarantee the rights of freedom of expression and information.
- Iraqi civil society organisations and other stakeholders should be engaged in the drafting of such laws.
- The NIC must reform regulations to simplify foreign investment flow.

JORDAN

The Internet was introduced to Jordan in 1995 and today's Internet market is highly competitive with sixteen Internet Service Providers (ISP) providing top quality, reliable broadband and WiMAX Internet services. Jordan also has three highly-competitive mobile operators which provide an extensive array of 3G mobile services. The Telecommunications Regulatory Commission (TRC) regulates both the Internet and Mobile industries.¹³⁰

There are no restrictions on the Internet in Jordan. Internet coverage, both wired and wireless infrastructure, is nationwide with more focus on dense areas (mainly the principle cities) and less on rural areas. The introduction of WiMAX and 3G in 2009¹³¹ increased geographical penetration through Internet access points and the rise of the Internet.¹³² The ISP market in Jordan is highly competitive with sixteen reported ISPs, many of which provide reliable services at competitive prices. Market forces continue to help the decline in Internet prices, encouraging Internet uptake and making Internet provision in Jordan more affordable.¹³³ Mobile operators are providing data package options at reasonable

prices to cover the largest portion of subscribers interested in purchasing such services.¹³⁴

Statistics on Internet penetration in Jordan vary. During the same period at the end of 2011, the Jordanian Department of Statistics (DoS)¹³⁵ reported a penetration rate of 34.9%,¹³⁶ while the Jordanian TRC¹³⁷ reported 50.5%.¹³⁸ This highlights, amongst many things, the lack of objective statistics on this matter, or of openness within governmental organisations. Online news sites are ranked as the preferred destination for around 70% of Jordanian Internet users, with music coming in at number two, and sports in third position. 72% of Jordanian Internet users are aged between 15 and 24 years.¹³⁹

The concept of "Internet Governance (IG)" in Jordan is not widespread. Some pillars of IG, such

130. http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-AR-2012-PDF-E.pdf

131. http://www.jordantelecomgroup.jo/jtg/Home/MediaRelations/News/jtg_3G_license/tabid/561/Default.aspx

132. <http://jordantimes.com/zain-jordan-boasts-1m-subscribers-to-3g-services>

133. http://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-AR-2012-PDF-E.pdf

134. <http://jordantimes.com/umniah-introduces-3g-services>

135. The Department of Statistics (DoS) was established in the late 1949 and assumed its activities in accordance with the Statistics Law No. 24 for the year 1950.

136. http://www.dos.gov.jo/dos_home_a/main/jorfig/2011/13.pdf

137. The Telecommunications Regulatory Commission (TRC) was established by means of the Telecommunications Law No. 13 of 1995, and its amending law No. 8 of 2002 as a financially and administratively independent jurisdictional body tasked with regulating the ICT sector. While it performs its duties independently of the Jordanian Ministry of Information and Telecommunications Technology (MoICT), it complies with the general policy of the Government of Jordan.

138. http://trc.gov.jo/index.php?option=com_content&task=view&id=index.php?option=com_content&task=view&id=2021&lang=english

139. <http://jordantimes.com/news-websites-most-popular-destination-for-jordanian-internet-users----study>

as security, e-government and infrastructure, are widely applied, whilst others are only partially implemented, such as Domain Name System (DNS) and IPv6. However, others, such as Open Data, Online Freedom of Expression, New gTLDs, and DNSSec, are still not applied at all. Furthermore, the Policy Development Process (PDP) in Jordan lacks a multi-stakeholder, bottom-up, consensus-driven approach. This is due to the fact that the majority of government entities enforce laws passed by the Ministerial Cabinet, with royal approval but without public consultation.

FREEDOM OF EXPRESSION (FOE) AND THE CURRENT SITUATION OF INTERNET OPENNESS

In 2012, the Independent London-based public policy organisation, the Legatum Institute, ranked Jordan 133 in terms of Personal Freedom.¹⁴⁰ The Jordanian government still prohibits citizens from what they consider to be 'crossing redlines'. This includes, criticizing the ruling family, making comments deemed to offend Islam (the official religion of the state), diminishing the prestige of the State, or harming international relations. These are very general and ambiguous laws which can be used to detain individuals as suits various elements of the state apparatus and, as and when it pleases the regimes' agenda. Though the recent Arab revolutions annulled the law prohibiting Jordanians from defaming government officials and institutions, those caught crossing redlines are still interrogated by the Jordanian General Intelligence Department (GID) and potentially detained.¹⁴¹ This has led

to many great thinkers and political opposition leaders fleeing Jordan in the hopes of finding a land which allows them to express their beliefs without fear of discrimination. Consequently, it is reported that 94% of Jordanian journalists practice self-censorship.¹⁴²

Prior to the evolution of the Internet in daily Jordanian lives, redline crossings were limited to traditional media, appearing on satellite TV channels, in international newspapers or through opposition leaders. This limited the risk of prosecution from the State as citizens were only consumers of content. However, the post-Internet individual has become a producer of content, and is now in direct conflict with the State. For example, Ahmed Oweidi Al-Abbadi and Abdul Salam Al-Mualla are two Jordanian opposition leaders and founders of the Jordan National Movement in the USA.¹⁴³ The *Al-Jazeera* news channel, a satellite TV news channel broadcasting from Qatar, caused unrest in relationships between Jordan and Qatar by broadcasting news criticizing the monarch and his family.¹⁴⁴ *The Arab Times*, a controversial newspaper published in the USA, is banned in Jordan for its critical tone towards the Jordanian monarchy.¹⁴⁵ Laith Shubeilat, a reformist opposition figure in Jordan, has been detained and allegedly tortured on several occasions for opposing the ruling family and the government.¹⁴⁶ These examples, and more, reflect ongoing concern regarding the right of the Jordanian citizen to freedom of expression.

142. <https://www.goethe.de/ins/jo/amm/prj/ema/far/job/enindex.htm>

143. <http://www.jordannationalmovement.com/>

144. http://www.atimes.com/atimes/Middle_East/DH15Ak01.html

145. <http://old.openarab.net/en/node/349>

146. <http://shubeilat.com/about/>

140. <http://www.prosperity.com/CountryProfile.aspx?id=400>

141. <http://www.hrw.org/world-report-2011/jordan>

The Arab revolutions of late 2010 put Jordan, like many of its neighbours, on high alert. In order to avoid the situations spilling over into Jordan, a new government was formed with verbal instructions to fight all forms of corruption and launch a solid reform process through the establishment of a “National Dialogue Commission”. In December 2011, high profile arrests were made, including that of Amman’s mayor, Omar Maani, who was charged with fraud. In February 2012 Mohammad Dahabi, the former director of Jordan’s intelligence service, was taken into custody on charges of money-laundering, and was later sentenced to thirteen years’ imprisonment. These incidents and others were the beginning of a new era for some Jordanians. More public criticisms of the monarch, his family, and the government were made online and in traditional media. Jordanians took to the streets in protest on a weekly basis, requesting that more reformative action be taken and that the government deal with the protests cautiously.

This said, sixteen assaults were registered against journalists during the first quarter of 2012¹⁴⁷ and twenty-four during the period 1 May – 1 September, 2012.¹⁴⁸ In March 2012, four Jordanian activists participated in a sit-in calling for increased job opportunities for the unemployed, but did it in a manner that was not deemed appropriate by the State. As a consequence, they were imprisoned.¹⁴⁹ In

147. <http://jordantimes.com/16-assaults-against-journalists-registered-in-first-quarter>

148. <http://jordantimes.com/24-assaults-against-journalists-registered-over-past-four-months----report>

149. <http://www.freedomhouse.org/article/jordanian-activists-detained-criticizing-king-abdullah-ii>

April 2012, twelve protesters were referred to the State Security Court for insulting the monarch and threatening national security.¹⁵⁰ In July 2012, Jordan’s then Prime Minister, Dr. Fayez Tarawneh,¹⁵¹ requested suspension of the Jordanian TV satellite channel JO-Sat for airing a show entitled *Blaming the Government*, and of the GID for slowing down the reform process.¹⁵²

Jordanian expatriate citizens are able to use the Internet in an enabling way which is not available to Jordanian citizens living within the country. Internet users in Jordan are limited by stringent laws limiting their freedom of expression through fear of detention. In February 2012, female blogger Enass Musallam was stabbed, allegedly because she criticised a member of the royal family on her blog.¹⁵³ The Omani student of Jordanian law, Ammar Al-Mamari, famously blogged from Jordan about the repression of the Omani government, and events took a twist in August 2012 when Jordanian government officials contacted his parents in Oman, requesting that their son stop his writings, or face being deported according to Freedom House.¹⁵⁴ During the second half of 2011, Google received ten requests from the Government of Jordan to remove online content. Such requests are either made by government officials in the Royal Court or by the Jordanian Intelligence Department.

150. <http://jordantimes.com/between-defamation-and-free-speech-the-need-to-define-the-red-lines>

151. In Jordan, the king appoints the prime minister based on geographical diversity, and the prime minister chooses the cabinet.

152. <http://www.freedomhouse.org/article/clampdown-government-critics-augurs-poorly-jordan>

153. <https://cpj.org/2012/02/in-jordan-blogger-stabbed-after-criticizing-the-royal.php>

154. <http://www.freedomhouse.org/article/omani-blogger-threatened-deportation>

Google declined to remove any content on the grounds that it did not violate Google's online content publishing policies.¹⁵⁵ In January 2010, the Court of Cassation enforced websites and electronic media to comply with the Press and Publication Law. However, implementing such a decision was beyond the jurisdiction of local courts because the majority of the websites were hosted overseas.¹⁵⁶ In July 2012, the government announced that it would amend the Press and Publications Law (PPL) to include amendments which covered cyberspace. The proposed legislation includes items that would hold online media accountable for comments posted by readers, require online media entities to archive all comments left on their sites for at least six months, require online media to register with and obtain a license from the PDP, thus forcing them to become a member of the Jordan Press Association, and giving the government authority to block sites that fail to comply.¹⁵⁷ On 17 September 2012, a royal decree passed the new amendments of the PPL.¹⁵⁸

NICHES OF AREAS OF IMPORTANCE WITHIN THE INTERNET LEGISLATION/POLICY

In Jordan, there has not been heavy investment in Free Open Source Software (FOSS). The Jordanian Ministry of Information and Communications Technology (MoICT) has

been attempting to deal with this situation as around 57% of software used in the past two years is pirated.¹⁵⁹ In 2010, the MoICT signed a Memorandum of Understanding (MoU)¹⁶⁰ with Ingres Corporation.¹⁶¹ The project targets local universities and has a mandate to make FOSS the software platform used within the government of Jordan (ministries and governmental entities).¹⁶²

The MoICT oversees the policy development of the Information and Communication Technology (ICT) sector. Policy is reviewed on an annual basis, taking into account feedback from the ICT industry (mainly the giant Telco operators), the latest international trends and best-practices suggested by international organizations such as the International Telecommunication Union (ITU). The draft policy of each coming year is drafted for review by the public via the MoICT's website. Feedback is accepted and incorporated and the final document is submitted for approval by the Ministerial cabinet. Once approved, the policy is enforced via the MoICT's regulatory bodies - the TRC and the National IT Center (NITC).¹⁶³ The Ministry ensures continuous improvement and stronger competition to and within the ICT sector by providing incentives in the form of discounts on

155. <http://www.google.com/transparencyreport/removals/government/JO/?p=2011-12>

156. http://www.huffingtonpost.com/daoud-kuttab/jordans-newssites-volunta_b_917809.html

157. <http://www.jpa.jo/english/JPALaw.aspx>

158. <http://jordantimes.com/royal-decree-endorses-press-law>

159. <http://www.microsoft.com/middleeast/press/Pages/Article.aspx?id=903>

160. http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100112005382&newsLang=en

161. Ingres Corporation is a leading open source database management company and pioneer of the New Economics of Information Technology (IT)

162. <http://jordanopensource.org/article/jordan-become-open-source-hub-middle-east>

163. <http://www.moict.gov.jo/ar-jo/%D9%85%D8%B1%D9%83%D8%B2%D8%A7%D9%84%D8%A7%D8%B9%D9%84%D8%A7%D9%85%D8%A2%D8%AE%D8%B1%D8%A7%D9%84%D8%A3%D8%AE%D8%A8%D8%A7%D8%B1.aspx>

annual service fees (such as spectrum allocation fees and international Internet fees) to those who fulfil the regulatory requirements with minimal annual violations. The Ministry also introduces new ICT services (such as 3G, 4G, and WiMAX) in the form of Tenders where interested providers are requested to submit strong proposals.¹⁶⁴

STATUS OF ACCESS TO INFORMATION, TRANSPARENCY, ACCOUNTABILITY, AND E-PARTICIPATION

Whilst Jordan was the first Arab country to officially endorse a law in 2007 which preserves the right to Access of Information (AoI),¹⁶⁵ loopholes¹⁶⁶ which prevent access to information and provide few guarantees to those seeking it, are abundant.¹⁶⁷ One such loophole contradicts the Press and Publication Law (PPL) of 1999. For example, Article 7 of the law prohibits public demand for information which has “religious, racial and ethnic discrimination or discrimination based on sex or colour”. Article 13 authorises officials not to disclose information related to State secrets and confidential documents stipulated in other legislation, thus contradicting the reason for devising such a law. In 2008, another amendment was added which stated

that journalists would be imprisoned if they violated the PPL. However, this amendment was overturned and never saw the light of day.¹⁶⁸ Further amendments to the PPL took place in September 2012, imposing greater restrictions to freedoms of expression online. Another loophole initiated an amendment, in September 2011, to the country’s Anti-Corruption Law. This amendment penalized the publication or dissemination of allegations of corruption without proof incurring fines ranging from USD 42,000–85,000. The law was rejected in January 2012.¹⁶⁹ In September 2012, a draft amendment was endorsed, the major item being to improve the representation of civil society organizations on the Information Council.¹⁷⁰

In August 2010, the Jordanian parliament passed a cybercrime law, specifically to penalize hacking and online identity theft. However, some provisions were identified as a means by which to further restrict freedom of expression online.¹⁷¹ For example, Article 8 of the law contained a vague definition of the posting of insulting comments (this Article was withdrawn in a subsequent Amendment). Article 9 prohibited “immoral content” - a vaguely-defined term. Article 12 banned the posting of information concerning Jordan’s national security, foreign relations, public order, or economy - information previously unavailable to the public. Article 13 gave the Attorney General full power to issue

164. http://www.jordantelecomgroup.jo/jtg/Home/MediaRelations/News/jtg_3G_license/tabid/561/Default.aspx

165. <http://www.giswatch.org/country-report/20/jordan>

166. For example, article 7 of the law prohibits public demand of information that has “religious, racial and ethnic discrimination or discrimination based on sex or color”. Article 13 of the law gives authority to officials not to disclose information related to state secrets and confidential documents stipulated in other legislations, thus contradicting the reason behind devising such a law.

167. <http://www.alarcheef.com/reports/englishFiles/accessToInformation.pdf>

168. <http://www.amnesty.org/en/region/jordan/report-2008>

169. http://www.khaleejtimes.com/darticlen.asp?xfile=data/middleeast/2011/September/middleeast_September568.xml§ion=middleeast

170. <http://jordantimes.com/cabinet-endorses-draft-amendment-to-access-to-information-law>

171. http://ifex.org/jordan/2010/09/03/cyber_crimes_law/

police warrants to search the office or home of anyone suspected of violating the law.

It has become a common trend in Jordan for website owners to receive phone calls requesting the take-down of content. Such phone calls are mainly initiated by government officials, security services, politicians, and prominent Jordanian figures. In February 2011, the national online newspaper *Amon News* was hacked after it refused to take down a joint statement by thirty-six prominent Jordanian tribesmen¹⁷² requesting reform. The joint statement was eventually removed by the hackers.¹⁷³ In March 2012, the *Al-Arab Al-Youm* newspaper was pressurized by the Royal Court to take down an article entitled “*We Will Not Live in a Stupid Man’s Robe*”. The article criticized the government for the way in which they were fighting corruption and unemployment and for how they had dealt with protests in some Jordanian cities.¹⁷⁴

In 2006, the Jordanian government launched its e-government services with the aims of transforming Jordan into a knowledge-based economy, and conducting public sector reform and utilizing technology as an enabler.¹⁷⁵ However, a United Nations survey conducted in late 2011 ranked Jordan’s e-government program at 98 out of 190, moving down from 51 at the end of 2010. Part of the e-government service is the introduction of e-participation. The Legislation and Opinion Bureau is the governmental body which oversees this initiative, and has a

172. Tribesmen in Jordan have always been known for their historic support to the monarch.

173. http://www.ifex.org/jordan/2011/02/11/ammon_news_hacked/

174. http://www.ifex.org/jordan/2012/03/26/article_censored/

175. <http://www.jordan.gov.jo/wps/portal/MyArabicPortal>

dedicated web portal for this purpose.¹⁷⁶ While the bureau receives comments from the public on drafts of new and amended laws published on the portal, it does not have a process in-hand to receive suggestions about new laws or amendments to existing laws (citizens writing new laws or proposing amendments to existing ones).

In 2008, The Jordanian Alliance for the Freedom of Information and Transparency (JAFIT) was born. The coalition consists of various stakeholders related to information dissemination – mainly media reporters and bloggers. It conducts campaigns and activities to promote the freedom of information and transparency. Some Jordanians believe that information transparency and accountability are the crux of large-scale reform.¹⁷⁷

THE IMPACT OF SOCIAL MEDIA ON CIVIL LIBERTIES

Statistics show that Jordan has approximately 2.5 million active Facebook accounts,¹⁷⁸ approximately 50,000 Twitter accounts (of which approximately 15,000 are active)¹⁷⁹ and approximately 212,000 LinkedIn accounts.¹⁸⁰ Several governmental ministries and offices maintain Facebook and Twitter accounts. Notably, Queen Rania and Queen Noor are known to be

176. http://www.lob.jo/List_LawsLegislations_Public.aspx?Page=Vote

177. <http://www.black-iris.com/2011/01/24/why-transparency-may-be-the-first-step-for-serious-reform-in-jordan/>

178. <http://www.socialbakers.com/facebook-statistics/jordan>

179. <http://jordantimes.com/twitter-study-points-to-declining-happiness-but-users-dont-plan-to-stop>

180. <http://www.socialbakers.com/countries/linkedin-in-country-detail/jordan>

active on social media sites including Facebook and Twitter.

Many Jordanian civil movement groups create social media accounts, mainly using the Facebook platform, to discuss topics of interest. In March 2011, a Facebook group named “*Youth of March 24*” was created with the aim of organizing a demonstration. The group demanded the resignation of Dr. Marouf Al-Bakhit, the Prime Minister at that time, reform of parliament, and trials of the corrupt.¹⁸¹ While the demonstration did go ahead, the government did not comply with the demands, as it remained undismantled. In February 2012, a Facebook group called “*Ensaf*” was created to promote Internet censorship, mainly blocking pornographic content.¹⁸² In April 2012, the “*No Internet Censorship in Jordan*” Facebook group was created to fight Internet censorship.¹⁸³ In August 2012, Queen Noor of Jordan tweeted on her Twitter page, expressing her dissatisfaction at the 2012 amended Press and Publication Law (PPL).¹⁸⁴

CONTENT FILTERING

Internet surveillance and monitoring surfaced as a major civil rights issue in March 2008, when the Jordanian Ministry of Interior Affairs issued new instructions to Internet café owners to install cameras in order to monitor users, register the Internal Protocol addresses of the café, register the users’ personal data, register the time of use, and register the data of websites explored.¹⁸⁵

While some activists did express their concern at such instructions, the majority of Internet café savvies were fine with them.

Prior to the PPL of 2012, *The Arab Times*¹⁸⁶ was the only online content to be filtered in Jordan. Their website had been blocked since 2001.¹⁸⁷ In 2008, strict censorship policies were implemented within the governmental network. Content related to general terms such as pornography, social media, audio/video streaming, and proxy websites/software, was all blocked. In mid-2010, a government source confirmed that a 30-day study had concluded that government employees spent, on average, 3 of their 7-hour work day surfing local online newspapers. As a consequence, the top fifty most visited online news sites were blocked within the governmental network. In late-2010, and under the next government, this ban was lifted, leaving other previously-blocked content blocked within the governmental network.

In early 2012, two civil society groups concerned with Internet content filtering were formed. The first group, “*Ensaf*”,¹⁸⁸ was in favour of filtering content concerned with pornographic content due to its violation of the teachings of Islam and the social norms of Jordan. The other group, “*No Internet Censorship in Jordan*”,¹⁸⁹ opposed content filtering on the grounds that

cafe-users-be-monitored

186. The Arab Times is a well-known Arabic newspaper based in the USA. While it started in 1986, it launched its online services in 1997. It is known for its criticism targeting Arab leaders and monarchs. It is blocked in many Arab countries such as Jordan, Kuwait, and Saudi Arabia.

187. <http://old.openarab.net/en/node/349>

188. <https://www.facebook.com/ensaf0>

189. <https://www.facebook.com/NoInternetCensorshipInJordan>

181. <http://www.bbc.co.uk/news/world-middle-east-12857360>

182. <https://www.facebook.com/ensaf0>

183. <https://www.facebook.com/NoInternetCensorshipInJordan>

184. <https://twitter.com/QueenNoor/status/240780558018412544>

185. <http://www.menassat.com/?q=en/alerts/3178-jordan-internet->

it would harm the Jordanian Information and Communications Technology sector.¹⁹⁰ In July 2012, the government of Jordan placed Internet censorship high on its agenda as part of the amended PPL of 2012. On 29 August 2012, and in opposition to the suggested amendments to the PPL, around two hundred Jordanian websites participated in a 24-hour blackout, displaying black screens as their main page.¹⁹¹ The high profile figure, Queen Noor of Jordan, tweeted on her Twitter page expressing her dissatisfaction at the amended PPL.¹⁹² On 17 September 2012, a royal decree passed the new amendments of the PPL with immediate effect.¹⁹³

CONCLUSION AND RECOMMENDATIONS

The introduction of smart phones has helped increase Internet penetration rates in Jordan. Internet Governance is not a widely-used concept. When it comes to Freedom of Expression, Jordan clearly has a long way to go as access to Information is highly restricted and e-participation has limited implementation. 2012 has witnessed a considerable number of human rights violations against reporters, bloggers and media outlets as the traditional “red line” boundaries have been publicly pushed.

The Press and Publication Law of 1999 and its subsequent amendments are seen to be one of the main obstacles behind the low levels of FoE, Access to Information, and e-participation. The new cybercrime law of 2010 has many loopholes which could restrict FoE online. Enforcing stringent Internet filtering in late 2012 is another highly controversial issue within the Jordanian Internet community. The unrest in the region, due to the Arab revolutions, is another factor affecting future development. The lack of understanding of key Internet Governance and the Policy Development Process topics are additional obstacles which must be tackled. In light of the above, the following recommendations would progressively change the status quo:

1. Amendment of the Press and Publication Law and the Cybercrime Law to ensure higher levels of FoE and better immunities for journalists, bloggers, and online Internet users. Such laws must comply with the international conventions on FoE and human rights. Amending such laws would encourage industry growth of local hosting services and data centres, thus enhancing further local content.
2. Reconsideration of the concept of enforcing Internet Content Filtering. Education and capacity-building are methods which must be explored further.
3. Provision of awareness and capacity-building programs on issues related to Internet Governance and encouragement of the multi-stakeholder, bottom-up, consensus-driven concept.

190. Jordan is dubbed as the Silicon Valley of the Middle East. In 2012, it was ranked as the 10th best city in the world to launch a tech startup (<http://www.bloomberg.com/news/2012-02-06/cohan-jordan-vc-firms-forging-mideast-silicon-valley.html>).

191. <http://www.globalpost.com/dispatch/news/regions/middle-east/jordan/120829/jordan-internet-blackout-protest>

192. <https://twitter.com/QueenNoor/status/240780558018412544>

193. <http://jordantimes.com/royal-decree-endorses-press-law>

4. Stronger local multi-stakeholder engagement at both regional and international forums such as ICANN, IETF, IGF, ITU, ISOC... and others, followed by the organisation of local events to update the public on what is taking place on regional and international stages.
5. The establishment of a multi-stakeholder organisation, which advocates the best interests of all Jordanian Internet users. Securing adequate financial resources could enhance the services provided by such an organization, which must play an influencing role in Press and Publication Law related to the Internet.
6. Enhancement and upgrading of services provided by the Jordanian e-government programme. This includes introducing services, which could assist in making the lives of Jordanian citizens easier (mainly e-services).
7. Further enhancement of the concept of Free Open Source Software (FOSS) and promotion of its usage. This will assist in reducing the cost of purchasing proprietary software and will further reduce the usage of pirated software.
8. The encouragement of research and development related to Internet Policy Development and Internet Governance.

SYRIA

Few can argue about the economic, societal and political transformations created by the Internet. In addition to its unprecedented power to facilitate trade and create knowledge-based economies and communities, the Internet has democratized communications and afforded the power of expression to all its users without discrimination. People can use the Internet to express their opinions, debate matters of public interest, and participate freely in the political discourse. These empowering features are warmly welcomed in environments that encourage participation and protect the individual's freedom of expression. Unfortunately, in places where these values are less cherished, the Internet's features, which promote self-expression and participation, are perceived as dangerous risks to the status quo, and are furiously resisted.

Freedom of expression and human rights do not seem to be well regarded in Syria's policy-making circles. The Syrian government has been accused by many international organizations of actively violating human rights and systemically oppressing freedom of expression. In its World Report of 2012, Human Rights Watch described Syria's human rights record as "poor", and accused the government of arbitrary detention, enforced disappearances, and torture. Amnesty International reported severe restrictions on freedom of expression in the country, and several cases of detention of human rights advocates.

Since 1963, Syria has been under emergency

law, which gave security forces unrestricted powers to detain civilians and repress civic freedoms. The emergency law was lifted in 2012 as part of several reforms designed by the government to contain the growing unrest in the country. The new reforms however failed to provide sufficient guarantees for the protection of human rights and freedom of expression. In the 2012 referendum, the country's parliament approved a new constitution which was hailed as an important reform initiative. However, many observers dismissed the significance of the changes and doubted that the new constitution would protect freedoms and human rights.

The Press Law of 2001 imposed significant restrictions on the freedom of the press, and prohibited coverage of many broad topics such as issues of national security. The law also gave the Prime Minister the power to reject or revoke licenses for journalists. Additionally, the Ministry of Information was given the power to ban foreign publications if deemed inappropriate. The law was amended in 2005 to include electronic publishing and websites. In 2010, the government approved a new law which allowed the government to arrest and prosecute publishers of online content in a criminal court.

INTERNET OPENNESS

The Internet constitutes a revolutionary democratizing medium for self-expression

and access to information. In Syria however, it is perceived as a threat to status quo, and was consequently actively controlled by the government. Internet traffic in the country is solely provided by the Syrian Telecom Establishment (STE), a government institution dealing with all telecommunication services. STE owns all telecommunications infrastructure in Syria, and is the exclusive owner of the international Internet gateways which link the country to the outside world.

Internet users in Syria face many restrictions, including, for example, blocking ports used for sending and receiving emails, blocking websites of a political nature, and restricting use of voice calls over the Internet. Many reports claim that the government actually intercepts web browsing and users' emails, and cite several cases in which Internet users were detained and faced trials because of their online activities.^{194,195}

These restrictions prevented many Syrian websites from establishing a presence inside the country. An advanced search on Google as of September 25th 2012 for all web pages under the country's top level domain (TLD) yielded 8,790,000 pages only. A similar search for the web pages under the Lebanese (.lb) TLD returned 9,540,000 pages (Syria's population is 5 times that of Lebanon). In order to secure better freedom and autonomy, most non-governmental Syrian websites opted to operate outside the country's borders, and are hosted on servers in other countries.

194. <http://opennet.net/research/profiles/syria>

195. <http://www.freedomhouse.org/report/freedom-net/2012/syria>

Other means of access to the Internet, such as Internet Cafes, are also strictly controlled. The government requires operators of Internet Cafes to obtain a photocopy of the ID cards of their visitors before they are allowed access.¹⁹⁶

No clear rules and policies exist for the blocking of websites, and many popular websites (including the Arabic Wikipedia) are banned. The OpenNet Initiative reports pervasive filtering of political web content, and that blocking spans a range of unpublished categories.¹⁹⁷ In 2001, Reporters Without Borders placed Syria among the 12 "enemies of the Internet" (countries which, according to the organization, restrict their citizens' freedom of information and curtail their access to the Internet).¹⁹⁸

INTERNET LEGISLATION AND POLICY

In 2010, the Syrian parliament approved a bill proposed by the Prime Minister to regulate Internet communication.¹⁹⁹ The law intends to impose more restrictions on online publishing and expression over the Internet. It grants authorities the right to detain online journalists, and seize their equipment if the government is apprehensive about the content published on the Internet. Under the provisions of the new law, journalists are tried in criminal courts rather than civil courts. Many believe that the new law will give rise to even more intense criticism of the government.

196. <https://www.nytimes.com/2008/03/25/technology/25iht-media.4.11415911.html>

197. <http://opennet.net/research/profiles/syria>

198. <http://en.rsf.org/beset-by-online-surveillance-and-12-03-2012,42061.html>

199. <http://www.syria-today.com/index.php/december-2010/688-news/13090-new-e-law-sparks-debate-among-web-journalists>

The Syrian president issued Decree No. 17, 2012 to regulate communications over the Internet and combat cybercrime.²⁰⁰ The decree was intended to establish the legal basis for the fight against cybercrime, but it also included several provisions which are perceived as threats to freedom of expression over the Internet. For example, the decree requires all Internet Service Providers (ISP) to retain all information posted by their users, and store traffic information which facilitates the identification of users. Another provision mandates that owners of websites publish their real identities and addresses. Article 13 of the decree states that high penalties can be levied if the cybercrime affects the government or public safety.

FREEDOM OF SPEECH ON THE INTERNET IN SYRIA: CHALLENGES AND LIMITATIONS

The Internet has always been perceived by the Syrian authorities as a tool which could facilitate self-expression and enable communications between citizens inside and outside the country. This probably explains why the Internet was very late to enter the country. It was not until the year 2000 that some Syrians were able to access the web (mostly government agencies and foreign embassies). Authorities felt uneasy about allowing access to the new medium without having the technology to enable surveillance and interception of users' activity and traffic.

The 2012 Freedom House report on Internet Freedom gave Syria a mark of 83 on its Internet Freedom Index (where 0 means most free, and

100 means least free).²⁰¹ The report cites tight controls maintained by the regime over ICTs, and claims that costs for Internet access constitute a major obstacle to access. For example, the cost of a 1Mbps ADSL connection to the Internet as of October 2012 is 1,400 Syrian Pounds (around \$20), representing 10% of the average monthly per capita income. The same report also documents extensive filtering and blocking of online websites. Internet users are forced to find solutions to circumvent government blocking and surveillance, whilst the government makes all efforts to prevent these tools and technologies from operating successfully.

Mounting evidence suggests that the Syrian authorities have actively pursued surveillance and monitoring technologies to track their citizens' activity on the Internet. For example, the California-based technology company Blue Coat, acknowledged that the Syrian government has used some of its products to censor Internet activity.²⁰² Other reports claim that the German firm Siemens has sold surveillance equipment to several Syrian telecom operators.²⁰³ An Italian company, Area Spa, was accused of building an elaborate surveillance system to intercept and monitor email traffic flowing through the country.²⁰⁴

Many countries, including the United States and the European Union, have imposed sanctions

201. <http://www.freedomhouse.org/report/freedom-net/2012/syria>

202. <http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html>

203. <http://www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html>

204. <http://www.bloomberg.com/news/2011-12-01/european-union-bans-exports-to-syria-of-systems-for-monitoring-web-phones.html>

200. <http://sana.sy/ara/2/2012/02/09/399498.htm>

on the export of surveillance technologies and equipment to Syria. However, these technologies seem to find their way into the country through alternative channels.

For Syrians, expressing opinions online can have severe and unpredictable consequences, including arbitrary detention and trial. With the lack of transparency surrounding the detention circumstances in the country, it is very difficult to determine the number of citizens and activists who have been arrested because of their activities on the Internet. Most Syrians believe that even simple online activities could result in them becoming targets for arrest, and the numbers of those in detention because of online activity are in the tens of thousands. Well-publicized cases include the arrest of blogger *Anas Maarawi*, as well as civil rights advocates *Mazen Darwish* and *Razan Ghazaawi* (from the Syrian Center for Media and Freedom of Expression). Some activists were even detained for years before the start of the Syrian uprising in 2011, including *Tal Al Mallouhi* who was arrested by security forces in 2009. She was then convicted on espionage charges.

ACCESS TO INFORMATION

It is difficult to imagine access to information flourishing in Syria where citizenship rights have little regard. The country has long suffered from very high levels of corruption, which placed it in the 129th rank among 183 countries on Transparency International's Corruption Perceptions Index of 2011.²⁰⁵ This wide spread corruption is nurtured by a severe lack of transparency, creating ample opportunity for corruption.

205. <http://www.transparency.org/country#SYR>

Freedom of information is a universally recognized fundamental human right, and the government is obliged to protect and ensure their citizens' have access to information. Many countries have institutionalized these obligations by adopting legislations that ensure free access to information, which is considered a great tool with which to hold governments accountable and prevent abuse of power. Syria has no specific freedom of information legislation, thus indicating that the Syrian authorities lack the desire to share information. This is highlighted in many high profile events, including claimed investigations into torture of citizens. The case of *Maher Arar*, the Syrian-Canadian citizen who was imprisoned by the Syrian authorities for 13 months, is a striking example. *Mr. Arar* was allegedly tortured during his imprisonment, although the Syrian authorities deny these allegations.²⁰⁶

The government frequently opposes the principles of access to information by imposing complete bans on foreign media reporters, or by preventing coverage of specific events (either by media outlets or citizen journalists). One report puts the impact of the lack of access to information as "ensuring that energy is exhausted in the search for information rather than in any more productive pursuit of justice".²⁰⁷

During the recent crisis, the Syrian authorities were widely accused of using different techniques to block access to information, including jamming satellite signals for news broadcasters which do

206. http://en.wikipedia.org/wiki/Maher_Arar

207. Walls of Silence: Media and Censorship in Syria, <http://www.article19.org/data/files/pdfs/publications/syria-walls-of-silence.pdf>

not side with the government's version of the story, including the BBC, France 24, Deutsche Welle, Voice of America, Al Jazeera and Al Arabiya.²⁰⁸ There is also blocking of opposition and political websites, and intercepting of voice and electronic communications and spying on the online activities of citizens.

TRANSPARENCY AND ACCOUNTABILITY

All of the previously mentioned factors (lack of freedom of information, lack of an appropriate legal and regulatory framework, and lack of respect of citizen rights) contribute to an environment in which transparency and accountability suffer greatly. It has even been argued that the nonexistent of transparency and accountability played a major role in igniting the civil uprising against the regime. It should be noted that Syria has remained under emergency law since 1963, and despite the law itself being lifted in 2011 in response to the uprising, it was quickly replaced by a vague and ambiguous anti-terrorism law which can be broadly interpreted and used to the same ends as its predecessor.

In an attempt to embrace e-government as a means by which to improve transparency and quality in public service provision, the Syrian Ministry of Communications and Technology (MoCT) launched an initiative in 2009 to develop a comprehensive strategy for e-government in the country.²⁰⁹ The Ministry also developed the Syrian e-Government Interoperability Framework (SyGIF) to facilitate the integration of different

services provided by different government agencies. The strategy states that the vision of the e-government initiative is to "provide excellence services to beneficiaries through improving the efficiency, productivity and transparency of government work, and provide comprehensive electronic services, available through multiple channels, while protecting private information". However, little information exists regarding the uptake and utilization of e-government services by Syrian citizens. The frequent disruption of the Internet connectivity in several parts of the country during the recent uprising poses additional challenges when it comes to the viability of such initiatives within the current political environment.

E-PARTICIPATION

The tense relationship between Syrian citizens and their leadership resulted in a significant lack of trust between the two parties. On one hand, the government does not feel obliged to ensure free access to information for its citizens, or guarantee the application of the rule of law and fight corruption. On the other, citizens have a general feeling of neglect, and that the government does operate with their interests at heart. This is also reflected in very low levels of civic participation.

The few attempts to create a more inclusive public sphere, such as the "Manifesto of the 99" signed by a group of Syrian intellectuals and activists, and the many forums of the Damascus Spring, were faced by more repression by the regime, and several participants were arrested and imprisoned.

It is not surprising then that the 2010

208. <http://www.montrealgazette.com/news/Syria+suspected+jamm+ing+news+broadcasts+Europe/7426394/story.html>

209. <http://www.moct.gov.sy/moctr/?q=ar/node/218>

E-Participation Index placed Syria in the 157th (last) rank, with an index value of 0.0143.²¹⁰ Some might argue that e-participation could provide a viable alternative to actual participation in the civic sphere, particularly for disadvantaged or underrepresented groups. However, the wide suspicion among the public of the government surveillance and control over the Internet prevents them from utilizing this medium to engage in the public discourse.

Several efforts were made in the hope of contributing to the reform of governmental institutions by means of providing e-government services, mostly led by international development organizations. The Syrian E-Government Initiative, launched in 2008 by the United Nations Development Programme (UNDP), is probably the most significant. These efforts, however, seem to have had very limited impact and acceptance among Syrian citizens. The perceived lack of interest and seriousness on the government's behalf regarding real reform and transparency is the most probable source of the public resistance. Many Syrians believe that the current governmental system is immune to reform, and must be fundamentally transformed to be able to respond to their ambitions and aspirations.

THE IMPACT OF SOCIAL MEDIA ON CIVIL LIBERTIES

The widespread use of social media in the Arab revolutions in Tunisia, Egypt and Yemen

have led many to believe that these emerging technologies can play an important role in empowering citizens and supporting civil liberties. It is important to understand the role of these different technologies as enabling tools for communication and self-expression which would support civil liberties, particularly in the Syrian context where other means of communications and expression are dominated by government control. One should however, not overstate the role of social media in a way that overshadows the actual, on the ground struggle for civil liberties.

In Syria, social media plays an important role in opening up new platforms for self-expression, creating channels for communication and facilitate reporting on emerging stories and events from citizen journalists on the ground. Syrians have experimented with social media tools since their emergence, starting with online discussion forums and blogs which were utilized to discuss and debate issues related to increasing personal liberties and pushing for transparency and accountability in the country. Most pioneers of these mediums used their actual names and identities to test the reactions of the authorities. Unfortunately, the response was quite harsh, and the detention and forced exile for many activists demonstrated how resistant the government is to discourse surrounding openness. Most activists now use pseudo-identities to enable them to communicate and express freely on the web.

One disadvantage of social media within this context is the fact that it can be easily used by authorities to track activists and their actions, which may result in more arrests and oppression. Authorities can, for example, force an activists to

210. More than one country can share the same rank on the E-Participation Index. Syria shares the last rank with several other countries, including Senegal, Namibia, and the Democratic Republic of Congo.

give up their account passwords to social media platforms like Facebook, and use these accounts to monitor the activists' communications and activities with others, and to entrap other members of their network.

CONTENT FILTERING

A study by the OpenNet Initiative found filtering of online content of political nature in Syria to be pervasive.²¹¹ The same study also indicates high and consistent levels of filtering and blocking of Internet security tools (tools used to circumvent government filtering and interception, like proxy servers and Virtual Private Networks VPNs). This type of filtering and surveillance resulted in very high levels of self-censorship among citizens.

Some network equipment obtained by the Syrian authorities is believed to be used for what is termed Deep Packet Inspection, a technique in which all packets passing through the Internet infrastructure pipes are sniffed and inspected to resemble the original communication. This would allow authorities to obtain copies of email communications, intercept online voice and instant messenger conversations, and track activities on social networks. The equipment from Blue Coat mentioned earlier is believed to be capable of Deep Packet Inspection. Another French company, Qosmos, was accused by the International Federation of Human Rights (IFHR) and the League of Human Rights (ILR) of supplying its Deep Packet Inspection technology to the Syrian regime. The company has denied these claims.²¹²

In conclusion, the evidence from Syria suggests a grim picture for freedom of expression in general, and for Internet openness in particular. The government seems to be engaged in active surveillance and monitoring of its citizens through all means of communication, and the Internet is no exception. The public sphere cannot function properly as a forum for citizen participation and contribution until the essential basic freedoms are guaranteed and protected by the rule of law. These include freedom of expression, protection of privacy and private communications, and respect for human rights. Only when citizens feel free and secure to voice their concerns and express their opinions will they be willing to actively engage in and contribute to forming the future of their country. An open and accessible Internet is an important ingredient which can facilitate participation, and urgent action at the policy making level must be taken to create the prerequisite environment for openness, transparency and engagement to thrive.

RECOMMENDATIONS FOR POLICY MAKERS

- Establish a clear and robust legal framework for access to information by adopting laws that ensure citizens' access to information. Requests for access to information should be governed by an independent entity free of government influence and control.
- Review existing laws and regulations to ensure that their provisions can be properly interpreted and eliminate areas that can be broadly utilized to repress access to information.

211. <http://opennet.net/research/profiles/syria>

212. <http://www.qosmos.com/qosmos-position-on-recent-claims/>

- Review the Press Law of 2001, the Internet Publishing Law of 2010, and the Communications over the Internet and Cybercrime decree (No. 17, 2012) to eliminate the restrictions imposed on freedom of expression online and on the Internet.
- Cease the detention of journalists and citizens on the grounds of expressing their views and opinions.
- Cease the practice of blocking websites based on their content, and initiate a public consultation to formulate clear, unambiguous rules to control censorship over the Internet.
- Cease the practice of Internet traffic interception for Syrian citizens and residents, and mandate a court order to be issued before any such activity.

TUNISIA

As a country which has transitioned from filtered to unrestricted Internet, Tunisia is a very unique case. Filtering systems were removed just after 14 January 2011 – the date on which the former Tunisian president Ben Ali, fled the country. To many Tunisians, this date symbolises the beginning of an ongoing democratic transition in response to Tunisian citizens’ aspirations for freedom, democracy and social justice. The Internet played a particular²¹³ role during that revolution and is part of the democratic transition. However, current Internet openness is a fragile situation with the possibility of a return to the previous status quo. Tunisia was previously listed several times in indexes such as the Opennet initiative, Reporters Without Borders (RSF) and Freedom House ‘freedom of the net’, which list countries implementing Internet censorship and at times labelled an enemy of the Internet.

An important milestone of the transition was the first free democratic election. It brought about a Constituent Assembly with the purpose of drafting a new Constitution. The previous Constitution, passed in 1959 and amended several times since, was suspended, and interim executive power acted through the decree of law. The drafting of a constitution is an opportunity to advocate the inclusion of strong legal provisions, which guarantee freedom and human rights according to international conventions such

213. Responding to that needs a study and it is quite controversial, the author prefers not taking position on that matter

as the United Nations Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). However, the new constitution is still in draft form and remains unclear. There have been difficulties²¹⁴ in its formulation, and its completion has been delayed.²¹⁵

This new political phase sees the increasing participation of social actors concerned with civic affairs, and the rise of debate concerning the transparency and accountability of government actions via Opengov and Opendata. The Internet is a critical tool for increasing civil participation, particularly via social media.²¹⁶

This report aims to illustrate the current Internet situation in Tunisia, with a focus on citizenship and Human Rights. Points to be considered include:

- Current Internet openness and the Tunisian Internet system as a critical means for democratization and political dialogue;
- The current situation around freedom of expression, its challenges and

214. <http://en.rsf.org/tunisia-cautious-welcome-for-pledge-that-12-10-2012,43535.html>

215. The election was held in 23 October 2011 and there was agreement between several political parties prior to the election that the Constituent Assembly presents a constitution by 23th October 2012

216. There is conflation between Internet, web and social media for many users and those terms may be used to indiscriminately

limitations;

- Opendgov and Opendata system positions, with specific focus on access to information, transparency and accountability and citizen's participation in political processes;
- The impact of social media on civil liberties;
- E-filtering;
- Analysis of Internet Governance in the Tunisian context from a human rights perspective;
- Recommendations to ensure an open and free Internet, and a multi-stakeholder participation process influencing Internet driven by the needs of citizens.

THE INTERNET: BETWEEN THE STATUS QUO AND CHANGE

In November 2005, Tunisia hosted the second phase of the World Summit on the Information Society (WSIS). This led to a set of principles known as the 'Tunis Agenda for the Information Society'.²¹⁷ This Agenda maintained the need for multi-stakeholder participation from government, the private sector and civil society, in Internet policy-making. There was no real follow-up on or commitment to these principles until 2011, and the former regime maintained heavy content control.

However the Agenda is an ongoing process. The first Tunisian Internet Governance Forum (TIGF) meeting was held in September 2012.²¹⁸ It resulted

in the creation of a secretariat and a national multi-stakeholder advisory group. Unfortunately, there was a lack of civil society representation at the meeting.²¹⁹ Having replicated the global IGF structure, some have also argued that it may add complexity to much-needed flexibility. Such a forum should be an open space for debating Internet Governance issues and moving toward recommending Internet policies at national level, as well as shaping Tunisia's position in international forums. However, such replication does give the national forum some formalisation.

In an attempt to be more open, the current Ministry of Information and Technologies of Communication (MoIToC) published its agenda on Information and Communications Technologies (ICT) up to 2013.²²⁰ This included action to end Internet filtering practices and restructuring both the Tunisian Internet Agency (TIA) and the National Authority for Telecommunications (NAFT). However, there remains a lack of open consultation regarding Internet policy and legislation, as well as a lack of commitment to the multi-stakeholder process in the reform of current laws and regulations.

The Tunisian government pledged to ensure the continuance of online freedom by:

1. in July 2012, signing the resolution²²¹ of the United Nations Human Rights

217. <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>

218. <http://www.mincom.tn/fileadmin/PDF/Compte-rendu-des->

Assises-dellIGFNationa-Fr.pdf (in French)

219. www.thd.tn/index.php%3FWEBSPPHERE/igf-tunisie-le-ministere-de-linterieur-au-premier-rang-la-societe-civile-sabsente.html (in French)

220. http://www.data.gov.tn/index.php?option=com_mtree&task=viewlink&link_id=136&Itemid=187 (in Arabic)

221. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.17_en.doc

Council (UNHRC) regarding the protection of human rights on the Internet and affirming ‘that the same rights that people have offline must also be protected online’, and;

2. joining the Internet Freedom Coalition (IFC) - a coalition of States initiated by Netherlands – at a conference in Nairobi in September 2012, and bidding to organise the next conference in June 2013.²²²

In addition to this, as a member of the International Telecommunications Union (ITU), Tunisia submitted a short proposal which recommended the inclusion of rights of freedom of expression and privacy in the International Telecom Regulations (ITR), with references to Article 19 of the UDHR, ICCPR and UNHRC resolution.²²³ This is a positive sign of coherence, which should be translated into national policies, and the reforming of current laws.

These pledges can be seen as ‘morally’ binding and exert pressure on current and future governments to respect such commitments. However, they are only general principles and, in order to be effective, must be implemented in national law. For example, the TIA, which was managing Internet filtering, is now facing multiple pressures from civil courts to apply Internet censorship to pornographic sites,²²⁴ arguing the case of child protection.²²⁵ Such censorship increases the risk of further restrictions, creating

a precedent for censorship on religious and social grounds.

There is also a significant risk of increased filtering on political grounds, and not necessarily through laws related to the Internet or telecommunications. For example, pages produced by the group *Takriz* were censored by a military court (as opposed to a civil court) on the grounds of defamation.²²⁶ This constitutes a threat to freedom of expression.

The pre-14 January legislation does not regulate content *per se*.²²⁷ Rather it became the responsibility of a third party, the Internet Service Provider (ISP), to filter what goes through their network. Such indirect regulation should be abrogated or it may also become a threat to freedom of expression. There is also a growing risk for regulation of social media space, in particular Facebook, since it is seen as an important medium and an online political forum.

OPEN GOVERNMENT: NEW OPPORTUNITIES AND POSSIBLE PITFALLS

Since January 2011 there has been an increasing demand from citizens to be involved in the political and decision-making processes. Public pressure for greater transparency and accountability of government and public administration is on the rise. Those demands include the constituent assembly work and constitution-drafting processes, which aim to outline the new political regime and the rights of Tunisian citizens.

222. <http://www.freedomonlinekenya.org/>

223. The document was leaked before the official publication of WCIT documents by ITU <http://news.dot-nxt.com/itu/wcit/c25>

224. http://www.inric.tn/INRIC_Rapport_final_en.pdf

225. <http://ati.tn/ar/index.php?id=97>

226. <http://www.article19.org/data/files/medialibrary/3014/12-04-03-ANAL-ICT-tunisia.pdf>

227. *Idem*

An informal group or network of individuals (with open membership) calling itself 'OpengovTN'²²⁸ advocates the use of social media (more specifically, Facebook)²²⁹ as a platform for discussion.²³⁰ It uses Facebook for information and advocacy purposes and for initiating projects with the collaboration of its members. The group also includes elected members of the Constituent Assembly from several political parties and organised a public campaign called *7ell* (which means 'open' in Tunisian dialect).

Another civil society organization called *Albawasala*²³¹ focuses mainly on following Constituent Assembly activity and publishing daily information about votes and attendance. It is currently taking legal action against the Assembly regarding their non-publication of committee minutes. The grounds for this action are lack of access to information, and to information which is in the public interest.²³² A similar initiative – *Marsad* – supported by Google, appears to have currently ceased its action for unknown reasons.²³³

The current government²³⁴ expressed interest in joining the Open Government Partnership (OGP)²³⁵ and in 2012 a delegation attended

the Brasilia conference.²³⁶ The previous government²³⁷ allowed access to information under Decree 41 of 26 May 2011²³⁸ and Decree 54 of 11 June 2011.²³⁹ These decrees represent the first milestones for citizen access to information and open data. However, they need to be placed into a broader, clearer framework and systematically enforced. The current government also launched an open data portal where documents issued by several ministries are available online.²⁴⁰ It set up another portal for combating corruption,²⁴¹ thereby demonstrating another step toward increased transparency. There are also some limited efforts by the current Constituent Assembly to publish its activities, committees' works and drafts of laws under discussion.²⁴² At local level, the small town of Sayada started its own initiative of Opendata²⁴³ and is publicising its activities and budget. Thus far, it is the only municipality to do so.

As these two decrees are temporary and of limited duration, they need to be translated into detailed and comprehensive law as soon as possible, following the vote on the constitution. Provision also needs to be made for accountability, transparency, openness and access to information. Moreover, resources and mechanisms will be required to enable such

228. <http://www.opengov.tn/> (in Arabic)

229. <https://www.facebook.com/groups/opengovtn/>

230. Facebook by the number of users in Tunisia is de facto the main platform for many Tunisians and is perceived as media, that cannot be ignored while that raise some question about the dependance to a commercial platform

231. <http://www.albawsala.com/fr> (in French)

232. <http://www.albawsala.com/fr/actu/50475d43b197de7ce3de4def>

233. <http://mejlis.tn>

234. Formed after the first elections in 23rd October

235. <http://www.opengovpartnership.org/>

236. <http://www.opengovpartnership.org/Brasilia2012>

237. Signed by the first interim president who held the power of issuing decree-law after constitution suspension

238. <http://www.cnudst.rnrt.tn/jortsrc/2011/2011f/jo0392011.pdf> (in French)

239. <http://www.cnudst.rnrt.tn/jortsrc/2011/2011f/jo0432011.pdf> (in French)

240. <http://www.data.gov.tn> (in Arabic)

241. <http://anticor.tn> (in Arabic)

242. <http://anc.tn> (in Arabic)

243. <http://villedesayada.tn/> (in French)

provisions. The decrees provide an adequate time-frame for the preparation of public administration to handle open data and access to information requests. They include provisions to enforce compliance with such requests and an appeals process through an independent 'administrative court'. There are also provisions for data protection and privacy which may justifiably limit access to data. Article 16 of Law 41 gives the administrative court the authority to make such decisions. However, limitations on the satisfaction of requests is unclear; intellectual property rationales are included in the same article.

In April 2012 the government, supported by inter-governmental organizations including United Nations Development Program (UNDP) and the World Bank,²⁴⁴ initiated a conference in Tunisia about Opendata and e-participation. A BarCamp Event called 'Citycamp' was held in Bizerte²⁴⁵ supported by World Bank initiatives engaging open data experts and partnering with ISOC Tunisia. This initiative focuses on local participation, working with the cities of Gafsa, Bizerte and Sfax. It analyses citizens' needs for local governance, recruits developers, encourages the emergence of 'Citizen technologists' communities and organises further citycamp events to increase awareness and education about open governance and open data.

The private sector has also been active in initiating and deploying an open data portal²⁴⁶

in order to experiment with the opening up of public and private data. Although this is mainly a technology-oriented project,²⁴⁷ the initiative also aims to provide a technology platform and to be an 'app store' for developers proposing applications using open data.

A strong focus on technological aspects (ie, apps) is noticeable amongst actors advocating open governance. Many appear to be driven by 'techno-determinism' – using technical solutions to fix all issues related to governance, transparency and accountability. However, they do so without a clear definition of citizens' requirements. 'Citycamp' carries out such work. Interest in open governance by governments is largely due to internal socio-political pressures and international loans requirements including the World Bank, the African Development Bank and the International Bank for Reconstruction and Development.²⁴⁸ However, due to private sector interests in open data, it is important to clarify regulations and limitations regarding the usage of public data for commercial purposes and to strengthen data protection and privacy laws.

In order for open governance to succeed, it requires a shift of perspective in government, administration and local authorities. This can only be achieved through projects increasing awareness, and an understanding by the population of their rights and needs to access information.

244. http://www.data.gov.tn/index.php?option=com_content&view=article&id=189&Itemid=204 (in Arabic)

245. <http://www.citycampsuntunisia.org/a-propos-du-citycamp-tunisia/> (in French)

246. <http://www.opendata.tn/>

247. <http://www.plattform.opendata.tn> (in French)

248. <http://www.cnudst.nrnt.tn/jortsrc/2011/2011f/jo0482011.pdf> (in French)

CONCLUSION

Although we acknowledge changes affecting freedoms and openness on the Internet in Tunisia, the situation may change due to the lack of a solid and sustainable legal framework and instruments guaranteeing and enforcing basic rights of freedom of expression.

The implementation of a mechanism to open Internet policy processes is still lacking. Civil society is not yet included in the policy process and needs resources and expertise to influence such processes.

To achieve freedom and development and to avoid over-regulation and control, a multi-stakeholder bottom-up and consensus-based approach should be applied to governance of the Internet and its management in Tunisia. It should focus on making citizen-oriented policies and prevent other interests from dominating. The Internet should be seen as an opportunity for development and growth, rather than as a threat to be over-regulated or controlled.

In addition to citizen participation in Internet policy-shaping, open governance initiatives should be reinforced to involve more citizens at both national and local levels. A more accessible and affordable Internet, along with the spread of digital literacy and education, can enable such participation on an equal basis and avoid a digital divide.

Finally, Tunisia has a great opportunity to make a dramatic change to its Internet environment and to move toward an open and free model, providing a medium for democratization, citizen participation and engagement, economic development and access to knowledge.

RECOMMENDATIONS

The Internet is a tool which can foster freedoms and democracy if used properly, although it is not an end in itself. Realising this is important in the construction of feasible and realistic national policies. These policies can be implemented respecting the principles included in the Tunis Agenda and aligned with International Human Rights in addition to economic development.

With regard to Internet policy-making and the legal framework, recommendations are:

- Including legal provision in the constitution with regard to the right to universal communication access (beyond the Internet) to prevent any attempt to re-establish excessive Internet filtering and surveillance methods.
- Ratifying and embracing international conventions and treaties including the Council of Europe Convention 108 regarding privacy²⁴⁹ and the Council of Europe Convention of Cybercrime to ensure more progressive legislation is implemented which is more oriented to the rights of citizens. It is also important to adopt the Charter of Internet Rights and Principles²⁵⁰ to provide a framework and guidance for national Internet policy-making.
- Focusing on capacity- and awareness-building at all stakeholder levels regarding Internet Governance

249. http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

250. <http://irpcharter.org/campaign/>

issues, on both international and national levels, in order to encourage multi-stakeholder policy processes. Capacity-building should aim to provide all parties with knowledge and toolkits to understand current and emerging issues.

- Encouraging national multi-stakeholder participation including international forums and spaces such as the IGF, the ITU, the International Corporation for Assigned Names and Numbers (ICANN), the African Network Information Centre (AFRINIC) and the United Nations Educational Scientific and Cultural Organisation (UNESCO) where Internet Governance issues should be encouraged.
- Creating an independent Internet Steering Committee at a national level with equal, balanced and diverse representation of all stakeholders and open membership (following the example of Brazil²⁵¹ and Kenya²⁵²). This committee should play an advisory role regarding Internet policies and provide recommendations to legislators regarding Internet-related legislation. It should also be able to assess implemented policies and evaluate their impact.
- Giving TIGF a prominent role in policy circles to institute an ongoing national debate regarding national and global Internet governance issues which include open governance and open

data processes, participation and accountability. The national IGF should be open to all interested parties and conduct regular open consultations with publication of the outcomes and recommendations of these meetings. It should be the primary space for raising awareness and enhancing participation. The Internet Steering Committee should play an important role in managing the national IGF.

- Restructuring national agencies managing Internet aspects e.g. the TIA, NIFT and the National Frequencies Agency (NFA). Their missions should be redefined using an open consultations process, requesting comments and creating adequate multi-stakeholder advisory groups within them. There should be particular focus on the TIA, which has taken action to become a full Internet Exchange Point (IXP) and Network Information Centre (NIC).
- Establishing open consultations and public comments regarding Internet policies to be conducted on- and off-line. The MoIToC should be responsible for conducting these consultations and partnering other organizations.
- Working on empowering and giving resources to existing and new agencies to enforce regulations related to privacy, data protection, competition, consumer rights and communications, so as to ensure the application of laws.
- Creating a system which ensures that any request for Internet filtering is for

251. <http://www.cgi.br/english/index.htm>

252. <http://www.kictanet.or.ke/>

limited cases according to the law, and should be made through the courts and not an administrative authority, whilst recognising UNHRD articles including Article 19²⁵³ and aligned with ICCPR in all requests.²⁵⁴

- Empowering citizens by educating them on their rights and responsibilities with regard to data protection and privacy, freedom of expression and guaranteed access.
- Encouraging research and academic work related to Internet policy by initiating postgraduate programs and providing grants and fellowships, together with establishing policy think tanks.

With regard to Internet infrastructure, recommendations are:

- Creating more affordable broadband access in all regions and ensuring that a universal, free basic access service is available to all citizens in order to spread digital literacy.
- Liberalizing the Internet market place by encouraging competition between ISPs.
- Increasing international connectivity and encouraging more peering and interconnection between national ISPs. The TIA has a central role to play as do national ISPs.^{255 256}

- Encouraging non-profit initiatives that provide free Internet access, including the liberalisation of spectrum management.
- Encouraging the localisation of content by suppressing all legal and economic barriers (i.e. local hosting) and pushing for open content and usage of open licensing (e.g. creative commons). Content hosting was hindered by tough regulation regarding third-party liability and should be dropped.²⁵⁷

With regard to Open governance, recommendations are:

- Capacity-building and intensive educational efforts within public administration and government ministries towards understanding OpenGov and Opendata principles and mechanisms.
- Building mechanisms to understand the citizens' needs and expectations regarding governance issues, at national and local level.
- Defining a final holistic legal framework regarding open governance and open data (with clear mention in the constitution) and providing the resources needed to enforce those laws (e.g. an independent instance on Opendata).
- Focusing on Internet access and on services matching real citizens' needs

253. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

254. <http://www2.ohchr.org/english/law/ccpr.htm>

255. <http://www.ati.tn/TunIXP/>

256. [http://www.mincom.tn/index.php?id=291&L=1&tx_ttnews\[tt_](http://www.mincom.tn/index.php?id=291&L=1&tx_ttnews[tt_)

[news\]=1329&tx_ttnews\[backPid\]=11&cHash=2eade78475](http://www2.ohchr.org/english/law/ccpr.htm) (in Arabic)

257. <http://www.article19.org/data/files/medialibrary/3014/12-04-03-ANAL-ICT-tunisia.pdf>

to avoid the rise of a digital divide and technology-oriented policy. Providing Internet public access, particularly in underserved regions, as a prerequisite to the use of Opendata services.

- Enforcing data protection and privacy laws related to Opengov and Opendata, accompanied by awareness campaigns regarding these initiatives.

Hivos | Raamweg 16 | 2596 HL | Den Haag | The Netherlands

+ 31(0)70 376 55 00 | www.hivos.org

Hivos is member of Alliance2015