Internet Filtering in the

Middle East and North Africa

OpenNet Initiative

Internet in the Middle East and North Africa

Countries in the Middle East and North Africa continue to invest in information and communications infrastructure and media projects as part of their strategies to develop the local economies and create employment.

Among the major examples are Jordan's plans to establish a free IT zone in Amman, which will give sales and income tax breaks to the software companies and business development firms based in the zone. The zone is part of a strategy designed to increase the number of Internet users from 26 percent to 50 percent. It aims to increase employment in the sector and to boost the sector's revenues from \$2.2 billion in 2009 to \$3 billion by end of 2011.1

In addition to existing regional hubs Dubai Media City and Dubai Internet City, the United Arab Emirates launched a new content creation zone to support media content creators in the Middle East and North Africa. The new Abu Dhabi-based zone aims to employ Arab media professionals in film, broadcast, digital and publishing. CNN, BBC, the Financial Times, Thomson Reuters Foundation, and Thomson Foundation are among the partners of the zone.²

At the same time, some countries have initiated efforts to develop Arabic Web content. In this regard, Microsoft is working on translation technology that would make the Arabic language more

accessible to Internet users as part of Qatar's Supreme Council for Information and Communication Technology's initiative to develop more Web sites with Arabic content.³

The number of Internet users is likely to continue to rise, especially with the introduction of technologies that overcome poor ICT infrastructure that hinders Internet access in the region. WiMAX, for example, was commercially available by end of March 2009 in Algeria, Bahrain, Jordan, Kuwait, Saudi Arabia and Tunisia, while operators in other parts of the region have started testing the service.4 Additionally, broadband markets are growing fast in Algeria, Egypt, Morocco and Tunisia, and commercial 3G mobile services have been launched in Egypt. Libya, Morocco, Sudan, Syria, and Tunisia.5

Demographic factors are also expected to contribute to the growth of Internet population. The Arab Media Outlook 2008-2012 says that, "Digital media will thrive in the Arab market because the market has a large, technologically accomplished demographic group—its youth—who are comfortable with it and will customize it to their own requirements." The report also revealed that, "over 50% of the population in Yemen, Oman, Saudi Arabia, Jordan, Morocco and Egypt are estimated to be currently less than 25 years old, while in the rest of the countries the under-25, 'net generation' makes up around 35% to 47% of total population."6

Liberalization of telecommunications markets has already taken place in several Arab countries. Most incumbent telecom companies in North Africa are already in private hands, with exception of Algerie Telecom, the privatization of which has been postponed due to the global economic crisis. However, experts say telecom liberalization in the Middle East and North Africa still lags behind the rest of the world in terms cost and efficiency, a matter which does not encourage direct foreign investment.

The Media Environment in the Middle East and North Africa

The Middle East and North Africa is one of the most heavily censored regions in the world. Human rights watchdogs and free speech advocacy groups continue to criticize the media restrictions and repressive legal regimes, and over the past few years, a great number of bloggers and cyber-dissidents have been jailed.

In April 2009, The International Federation of Journalists called for a radical overhaul of media laws in the Middle East, stating that the laws in most of the region's countries still permit the jailing of journalists for undermining the reputation of the state, the president, the monarch or the religion. Such laws have often been used to suppress reporting of corruption or scrutiny of government actions.9 This media environment created by authorities has been hostile to bloggers and online activism, resulting in a number of arrests across the region. In a list created by the Committee to Protect Journalists of the ten worst countries to be a blogger, four such countries (Egypt, Syria, Tunisia, and Saudi Arabia) were from the region.¹⁰

Internet and Media Regulations: The Debate

The last few years have witnessed an increase in the debate over media and Internet censorship in the region. Rifts between the censors and local and regional advocates of freedom of speech have intensified, and more voices continue to express concern about media regulations in the region.

Interestingly, while advocates in the region criticize the regimes for the repressive regulations, which limit freedom of speech online, some governments claim they arrest bloggers and online activists because they abuse what the regimes call "media freedom." In Egypt for example, the authorities arrested a blogger in May 2009 under the accusation of "Exploitation of the democratic climate prevailing in the country to overthrow the regime." The Cairo-based Arab Network for Human Rights Information deplored the charges and described them as a black comedy. 11 Another example of such a rift is from the Gulf countries, where the head of the Doha Centre for Media Freedom criticized Dubai Police for allegedly asking Google to censor YouTube. The head of the center was later criticized by Qatar officials as well as some journalists and was accused of endorsing pornography, 12 which is a sensitive topic in many Middle East and North African societies.

While it is common for Internet groups and online activists in the region to organize online campaigns to condemn online censorship and arrests of bloggers and online writers, other online campaigns which call for and support social censorship-mostly online pornography-have emerged in the past few years. For instance, an Arabic Web site called Ehjeb (Arabic for the verb "to block") is becoming increasingly popular, particularly among users of Web forums. The site offers to

facilitate blocking of Web sites by sending user-submitted URLs of questionable content to the censors in some of the region's countries. Also, some Internet users in North African countries where there is no social filtering have organized online campaigns to demand filtering of sexually explicit content.¹³

Pro-censorship advocates and anticensorship activists have also used the court system in their attempts to implement or remove censorship. For example, a judge in Egypt filed a lawsuit requesting the banning of 51 Web sites considered offensive. The court rejected the lawsuit in December 2007 and emphasized support for freedom of expression as long as the Web sites do not harm local beliefs or public order. In May 2009 however, a Cairo court ruled in favor of an Egyptian lawyer and ordered the Egyptian government to ban access to pornographic Web sites because they are deemed offensive to the values of religion and society.

In Tunisia however, a blogger challenged the Web filtering regime in the country by filing a legal suit against the Tunisian Internet Agency (ATI) for censoring the social networking site Facebook after it was briefly blocked in August 2008. The court dismissed the case in November 2008 without providing any explanation. These examples and cases illustrate how the fight over access control is taking different shapes and forms, and also indicate that different players will continue the debate and challenge each other.

Access Control in the Middle East and North Africa

Access control in the Middle East and North Africa is multilayered; governments and authorities use different measures to regulate Internet access and online activities. These measures include laws and regulations, technical filtering, physical restrictions, surveillance and monitoring, and harassments and arrests. Among the laws and regulations used to control access in the region are the press and publication laws, penal codes, emergency laws, anti-terrorism laws, Internet-specific laws, ISPs Terms & Conditions, and telecommunications decrees.

Press and Publication Laws, Penal Codes, Emergency Laws, and Antiterrorism Bills

Many countries in the region use restrictive press laws to regulate online publishing and traditional journalism. For example, censorship of online media and print journalism in Bahrain is exerted using the 2002 Press Law.14 Kuwait's 2006 Press Law allows imprisonment of journalists for making references to Islam that are deemed insulting, 15 or for articles seen as "against national interests." 16 Oman's 1984 Press and Publication Law authorizes the government to censor publications deemed politically, culturally, or sexually offensive. 17 Syria's 2001 Press Law sets out sweeping controls over publications printed in Syria. 18 And iournalists in Tunisia have been prosecuted by Tunisia's press code which bans offending the president, disturbing order, and publishing what the government perceives as false news.19 Yemen's 1990 Press and Publications Law subjects publications and broadcast media to broad prohibitions and harsh penalties.²⁰ The press law in Morocco has been used to suppress outspoken online writers.21

In addition to press codes, some countries often use penal codes to suppress journalists and online writers. Yemen's Ministry of Information declared in April 2008 that the penal code will be used to prosecute writers who publish on

the Internet content that "incites hatred" or "harms national interests."²² Syria's penal code criminalizes spreading news abroad.²³ Though the Bahraini government introduced in May 2008 amendments to the 2002 Press Law that eliminate prison sentences for journalists and prior censorship on publications, journalists can still be charged and jailed using the penal code and anti-terrorism law.²⁴

In addition to the use of penal and press codes, two countries-Egypt and Syria-both of which have been under emergency law for some time, have taken advantage of their status to punish individuals deemed threatening. Egypt's emergency law, in force since the declaration of the state of emergency in 1981, grants the administrative authority powers to search, arrest and detain individuals without the supervision of judicial bodies. Rights groups say that the uninterrupted application of the emergency law since 1981 has led to the emergence of a parallel legal system unchecked by ordinary judicial bodies.²⁵ Similarly, Syria uses the ongoing state of emergency (which began in 1963) to arrest media workers and journalists and political activists risk arrest at any time.²⁶ Morocco uses its anti-terrorism bill, passed following suicide bombings in Casablanca in 2003, to punish journalists. The bill grants the government sweeping legal power to arrest journalists for publishing content deemed to "disrupt public order by intimidation, force, violence, fear or terror."27

Internet-Specific Laws

Few countries in the region have introduced Internet-specific laws to regulate Internet activities; among them are the United Arab Emirates and Saudi Arabia. The UAE's 2007 federal cyber law criminalizes hacking, abusing holy shrines

or religious rituals, opposing the Islamic religion, transcending family principles and values, setting up a Web site for groups promoting programs in breach of public decency and order, and setting up a Web site or publishing information for a terrorist group under fake names with intent to facilitate contacts with their leadership, or to promote their ideologies and finance their activities, or to publish information on how to make explosives or any other substances to be used in terrorist attacks.²⁸

In January 2008, Saudi Arabia implemented 16 articles of new law on the use of technology. The law includes penalties of ten years in prison and a fine for Web site operators who advocate or support terrorism; three years and fine for financial fraud or invasion of privacy; and five years and a fine for those guilty of distributing pornography or other materials that violate public law, religious values and social standards of the kingdom. Accomplices of the guilty parties and even those who are proven to have only intended to engage in unlawful IT acts can receive up to half of maximum punishments.²⁹

Terms and Conditions of ISPs

Terms and conditions imposed by ISPs are also used to control access in some countries. In Oman for example, Internet use is regulated by the ISP Omantel's Terms & Conditions, which mandate that users "not carry out any unlawful activities which contradict the social, cultural, political, religious or economical values of the Sultanate of Oman or could cause harm to any third party" as any abuse and misuse of the Internet Services will "result in the termination of the subscription and/or in the proceedings of Criminal or Civil lawsuits against the Customer."30 Another example is Yemen where the terms and conditions set by the ISP

TeleYemen (aka Y.Net) prohibits "sending any message which is offensive on moral, religious, communal, or political grounds." TeleYemen reserves the right to control access to data stored in its system "in any manner deemed appropriate by TeleYemen." Section 6.3.3 cautions subscribers that TeleYemen will report "any use or attempted use of the Y.Net service which contravenes any applicable Law of the Republic of Yemen."³¹

Telecommunications Laws

Telecommunications laws are used to control what ISPs can and cannot host. In Algeria, for example, article 14 of a 1998 telecommunications decree makes ISPs responsible for the sites they host, and requires them to take "all necessary steps to ensure constant surveillance" of content to prevent access to "material contrary to public order and morality.32 Bahrain's Telecommunications Law of 2002 contains penalties for illicit use of the network, including the transmission of messages that are offensive to public policy or morals.33 And in Tunisia, the 1998 post and telecommunications law enables the authorities to intercept and check the content of email messages.34 Electronic surveillance such as filtering of email messages of government opponents has been reported in Tunisia.35

Surveillance and Monitoring

Measures to monitor Internet activities, particularly in Internet cafés, have been introduced in many Arab countries. In Algeria, security forces started raiding Internet cafés and checking browsing history of Internet users after terrorist attacks hit the country in April 2007. In April 2008, the security forces increased their monitoring and surveillance efforts of Internet cafés and Internet cafés were required to collect names and ID numbers of their customers and report this

information, together with any suspicious activities to the police.³⁶

Similarly, Jordan began in March 2008 increasing restrictions on the country's Internet cafés. Cameras were installed in Internet cafes to monitor users, and Internet café owners were required to register the IP number of the café, the users' personal data, the time of use and the data of Web sites explored.37 Additionally, Saudi Arabia's Ministry of Interior in April 2009 ordered Internet cafés to install hidden cameras and provide a record of names and identities of their customers.38 In Kuwait, Internet café owners also were required to maintain a record of customers' names and IDs, which they must submit to the Ministry of Communications (MOC) upon request.39

Some Internet café operators in Lebanon admit that they use surveillance computer software that enables them to monitor the desktops and browsing habits of their clients under the pretext of protecting the security of their computer networks or to stop their clients from accessing pornography. 40 In March 2008, the Syrian authorities ordered Internet café users to provide their names and identification cards and the times they use the Internet café to Internet café owners who will subsequently present them to the authorities. 41

In October 2007, police in Yemen ordered some Internet cafés to close at midnight and demanded that users show their identification cards to the café operator. Some Internet café owners use surveillance software to monitor the online activities of their customers and refuse access to clients who access pornography.

In August 2008, the Egyptian authorities imposed new monitoring measures by demanding that Internet café clients must provide their names, email

and phone numbers, before they can use the Internet. Once the data is provided, clients will receive a text message on their cell phones and a pin number that they can use to access the Internet.⁴⁴

In addition to the above measures, some countries impose physical restrictions on Internet cafés as part of the monitoring efforts. For example, Yemen⁴⁵ and Oman⁴⁶ require that computer screens in Internet cafés must be visible to the floor supervisor. No closed rooms or curtains that might obstruct view of the monitors are allowed.

Technical Filtering in the Middle East and North Africa

ONI conducted tests for technical Internet filtering in all of the countries in the Middle East and North Africa between 2008 and 2009. Test results prove that the governments and Internet service providers (ISPs) censor content deemed politically sensitive; critical of governments, leaders or ruling families; morally offensive; or in violation of public ethics and order.

Testing also revealed that political filtering continues to be the common denominator across the region. Many states in the Middle East and North Africa prevent their citizens from accessing political content or have blocked such content in the past. For example, Bahrain. Qatar, Jordan, the United Arab Emirates, Syria, Saudi Arabia, Morocco, Libya, and Tunisia have censored Web sites containing content critical of the governments and leaders, Web sites which claim human rights violations. and/or Web sites of opposition groups. Mauritania has briefly blocked the news Web site Tagadoumy, and Egypt has at some point blocked the Web site of the Islamic opposition group Muslim Brotherhood, as well as the Web site of the Labor Party's newspaper.

To one degree or another, the Gulf countries, as well as Sudan, Tunisia, Gaza, and Yemen, censor pornography, nudity, gay and lesbian content, escort and dating services, and sites displaying provocative attire. Also censored by most of these countries are Web sites which present critical reviews of Islam and/or attempt to convert Muslims to other religions. Some of these countries also filter Web sites related to alcohol, gambling, and drugs. Generally, the countries that implement political or social filtering also target to various degrees proxies and circumvention tools to prevent users from bypassing filters. Some of these countries also block online translation services and privacy tools apparently because they also can be used to access blocked content.

Regional Trends in Access Control

Internet censorship in the Middle East and North Africa is on the rise, and the scope and depth of filtering are increasing. Previous ONI tests revealed that political filtering was limited in some countries, but 2008-2009 results indicate that political censorship is targeting more content and is becoming more consistent. For example, previous tests found that Yemen temporarily blocked political Web sites in the run-up to the 2006 presidential elections, and Bahrain did the same ahead of parliamentary elections. However, 2008-2009 testing revealed that filtering in these two countries has been consistently extended to include several Web sites run by opposition groups or news Web sites and forums which espouse oppositional political views.

In the meantime, countries that have been filtering political content continue to add more Web sites to their political blacklists. For example, filtering in Syria was expanded to include popular sites such as YouTube, Facebook, and Amazon, as well as more Web sites affiliated with the Muslim Brotherhood Kurdish opposition groups. Another example is Tunisia, which added more political and oppositional content as well as other apolitical sites such as the OpenNet Initiative and Global Voices Online.

Social filtering is also increasing and is catching up with the continuously growing social Web. Most of the Arab countries were found to have started to block Arabic-language explicit content that was previously accessible. Interestingly, filtering of Arabic-language explicit Web content in the Middle East and North Africa is usually not as fast as that of other languages. ONI's investigation revealed that the US-based commercial filtering software used by most of the ISPs in the region does not pick up Arabic content as comprehensively as content in English.

Increases in filtering are the norm in the Middle East and North Africa, and unblocking is the exception. Of the few examples of unblocking of Web sites is Syria's restoration of access to Wikipedia Arabic, Morocco's lifting of a ban on a few pro-Western Sahara independence Web sites, and Libya's allowing access to some previously banned political sites. Sudan's filtering of gay and lesbian, dating, provocative attire and health-related sites was also more limited compared to previous test results.

Another regional trend is that more Arab countries are introducing regulations to make Web publishing subject to press and publication laws and requiring local Web sites to register with the authorities before they can go live. In Jordan, for example, the country's Legislation Bureau in the Prime Minister's Office issued in September 2007 a decision that Web sites and electronic press must comply with the provisions of the publications and publishing law and fall under the oversight of the Publications and Publishing

Department, which announced it would exercise immediate supervision and censorship.

Another example is Saudi Arabia, which announced in May 2009 plans to enact legislation for newspapers and Internet Web sites that will require Saudibased Web sites to get official licenses from a special agency under the purview of the Ministry of Information. Bahrain already has a similar system that requires local Web sites to register with the Ministry of Information.

Among the new trends in controlling access is the increase in incidents of hacking of opposition and dissident Web sites and blogs. Such incidents have been reported in Tunisia and Yemen. On the other hand, sectarian cyber war among different religious groups in the region, namely Shiite and Sunni groups, has occurred in the past few years. The cyber attacks managed to deface the Web sites of significant Shiite and Sunni organizations and individuals and in some cases the attackers managed to remove the content of some of these sites. Additionally, Israeli, Palestinian and Lebanese Web sites run by Hizbullah have been targets of attacks and hacking, especially during wars and conflicts.

Conclusion

Governments in the Middle East and North Africa continue to invest in media and IT projects, and at the same time are continuing to invest in censorship technologies to prevent their citizens from accessing a wide range of objectionable content. Also, while Western companies build ICT infrastructure necessary for development in the region, other Western companies provide the censors with technologies and data used to filter the Internet.

The censors in the region attempt to control political content using technical

filtering, laws and regulations, surveillance and monitoring, physical restrictions, and extra-legal harassment and arrests.
Filtering of content deemed offensive for religious, moral, and cultural reasons is pervasive in many countries and is growing.

Though many governments acknowledge social filtering, most continue to disguise their political filtering practices by attempting to confuse users with different error messages.

The absence of technical filtering in some countries in the region by no means indicates free online environments in those countries; surveillance and monitoring practices and extra-legal harassment from security agencies create a climate of fear used to silence online dissidents.

Many ISPs block popular politically neutral online services such as online translation services and privacy tools fearing that they can be used to bypass the filtering regimes. The censors also overblock Web sites and services such as social networking Web sites and photo and video sharing Web sites because of the potential for content considered objectionable.

More users in the Middle East and North Africa are using the Internet for political campaigning and social activism; however, states continue to introduce more restrictive legal, technical and monitoring measures, amid growing local and regional calls to ease restrictions and remove barriers to the free flow of information.

Author: Helmi Noman

NOTES

- Mohammad Ghazal, "Jordan, UAE firms in talks over free IT zone," The National, May 16, 2009, http://www.iordantimes.com/?news=1674
 - http://www.jordantimes.com/?news=1674 2.
- ² Keach Hagey, "Capital launches media zone to nurture young Arab talent," *The National*, October 13, 2008, http://www.thenational.ae/article/2008101
- 2/BUSINESS/13341341/1119/NEWS.

 3 Chris V. Panganiban, "Technology to promote
- Arabic online," *The Peninsula*, April 19, 2009,
 - http://www.thepeninsulaqatar.com/Display _news.asp?section=local_news&month=apr il2009&file=local_news2009041913642.x ml.
- 4 "Has the age of fixed wireless broadband services arrived in the Arab World? By end of March 2009, six Arab countries had eleven commercially launched," Arab Advisors Group, April 16, 2009, http://www.arabadvisors.com/Pressers/pre sser-160409.htm.
- 5 "2008 Africa Telecoms, Mobile and Broadband in Northern Region," *ChinaCCM*, December 2008, http://www.chinaccm.com/4S/4S16/4S16 07/news/20081205/111435.asp.
- ⁶ PricewaterhouseCoopers, "Arab media outlook 2008-2012," http://www.pwc.com/extweb/pwcpublicatio ns.nsf/docid/14D97CB491E2A59B852573 34000B8AAB.
- 7 "2008 Africa Telecoms, Mobile and Broadband in Northern Region," *ChinaCCM*, December 2008, http://www.chinaccm.com/4S/4S16/4S16 07/news/20081205/111435.asp.
- 8 Dana Halawi, "MENA telecoms need liberalization – Hasbani," The Daily Star, April 17, 2009,
 - http://www.dailystar.com.lb/article.asp?edit ion_id=1&categ_id=3&article_id=101067#.
- ⁹ International Federation of Journalists, "IFJ Demands Overhaul of Repressive Media Laws in the Middle East," April 29, 2009, http://www.ifj.org/en/articles/ifj-demands-

- overhaul-of-repressive-media-laws-in-the-middle-east.
- Committee to Protect Journalists, "10 Worst Countries to be a Blogger," April 30, 2009 http://cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php.
- "Egypt: new comic crimes written by the state security - Blogger in custody, on charges of exploitation of the democratic climate," The Arabic Network for Human Rights Information, May 14, 2009, http://anhri.net/en/reports/2009/pr0514-2.shtml.
- "A press row in Qatar -The limits to liberalization," The Economist, May 14, 2009, http://www.economist.com/world/mideastafrica/displaystory.cfm?story_id=13649580
- ¹³ "Users' Initiative to Block Web Sites," *OpenNet Initiative Blog*, October 24, 2008, http://opennet.net/blog/2008/10/users-initiatives-block-web-sites.
- ¹⁴ Bahrain Center for Human Rights, "Website accused of violating press code, BCHR concerned that move is aimed at silencing critical voices," September 2008 http://www.bahrainrights.org/en/node/244 6.
- 15 "Country Profile: Kuwait," BBC News, March 11, 2009, http://news.bbc.co.uk/2/hi/middle_east/co untry_profiles/791053.stm.
- Annual Report 2007", http://www.rsf.org/article.php3?id_article= 20767.
- ¹⁷ United Nations Development Programme, "Program on Governance in the Arab Region (UNDP-POGAR): Oman," http://www.pogar.org/countries/civil.asp?ci d=13.
- ¹⁸ Freedom House, "Map of Press Freedom 2008," http://www.freedomhouse.org/template.cf m?page=251&year=2008.
- ¹⁹ Committee to Protect Journalists, "Tunisia Report: The Smiling Oppressor," September 23, 2008,

- http://cpj.org/reports/2008/09/tunisia-oppression.php.
- 20 Yemen News Agency (Saba) Press and Publications Law, http://www.sabanews.net/en/news44000. htm.
- 21 "Appeal court overturns blogger's conviction," September 18, 2008, Reporters Without Borders, http://www.rsf.org/article.php3?id_article= 28603.
- 22 "Lawzi: Ma Yonshar fi Sahafat Al Internet Lan Yakon Ba'eedan A'n Al Mosa'ala bimojib Qanoon Al Oqobat" [Online journalism is subject to the penal code: Lawzi, Yemeni Minister of Information], Saba, February 3, 2008,
 - http://www.yemenna.com/vb/showthread.php?t=9502.
- ²³ Freedom House, "Map of Press Freedom 2008," http://www.freedomhouse.org/template.cf m?page=251&year=2008.
- 24 "Despite advances, journalists still face possible jail terms under prevailing laws, warns IFJ," International Federation of Journalists, June 12, 2008, http://www.ifex.org/en/content/view/full/9 4435/.
- ²⁵ Sarah Carr, "Journalists Challenge Egypt's Exceptional Laws at Seminar," *Daily News Egypt*, August 1, 2008, http://dailystaregypt.com/article.aspx?Articl eID=15464.
- ²⁶ Reporters Without Borders, "Syria Annual Report 2007," http://rsf.org/en-rapport163id_rubrique659-Syria.html.
- 27 "Background: The State of Human Rights in Morocco," Human Rights Watch, November 2005,
 http://bruy.org/reports/2005/morocco.1105
 - http://hrw.org/reports/2005/morocco1105/4.htm.
- 28 "UAE cyber crimes law," Gulf News, November 2, 2007, http://archive.gulfnews.com/uae/uaessenti als/more_stories/10018507.html.
- ²⁹ David Westley, "Saudi Tightens Grip on Internet Use," *Arabian Business*, January 26, 2008,

- http://www.arabianbusiness.com/509226-saudi-tightens-grip-on-internet-useoni.
- 30 Omantel, "Omantel Terms & Conditions," http://www.omantel.net.om/policy/terms.as p.
- 31 Y.Net, "Terms and conditions for Y.Net Service,"
 - http://www.y.net.ye/support/rules.htm.
- 32 Reporters Without Borders, "Internet Under Surveillance 2004 Algeria," http://www.rsf.org/article.php3?id_article= 10730.
- 33 Telecommunication Regulatory Authority (TRA) Kingdom of Bahrain, "Legislative decree no. 48 of 2002 Promulgating the Telecommunications Law," http://www.tra.org.bh/en/home.asp?dfltlng = 1.
- 34 "A textbook case in press censorship for the past 20 years," Reporters Without Borders, November 5, 2007, http://www.rsf.org/article.php3?id_article= 24264.
- 35 "Repression continues as Ben Ali marks 21st anniversary as president," *Reporters Without Borders*, November 7, 2008, http://www.rsf.org/article.php3?id_article= 29208.
- ³⁶ Fathiya Borowinah, "al-Jazaer: Ajhizat alamn tolin al-harb ala magahi alinternet liihbat masharee' khalaya irhabiya naemah" [Algeria: security services declared war on Internet cafes to thwart the projects of terrorist sleeper cells], *Al-Riyadh*, May 1, 2007,
 http://www.alriyadh.com/2007/05/01/artic
 - http://www.alriyadh.com/2007/05/01/article246175.html.
- 37 "Jordan: New Restrictions on Internet Cafes and Violating Privacy of Users," The Arabic Network for Human Rights Information, March 11, 2008, http://anhri.net/en/reports/2008/pr0311.s html.
- ³⁸ Helmi Noman, "Restriction on Internet use in the Middle East on the rise: Internet cafés in Saudi must install hidden cameras," OpenNet Initiative Blog, April 16, 2009, http://opennet.net/blog/2009/04/restrictio n-internet-use-middle-east-rise-internet-

- caf%C3%A9s-saudi-must-install-hiddencame.
- ³⁹ U.S. Department of State, "Country Reports on Human Rights Practices—2007," released by the Bureau of Democracy, Human Rights, and Labor, March 11, 2008, http://www.state.gov/g/drl/rls/hrrpt/2007/ 100599.htm.
- 40 "Baramij Malomatiya tadbut elaqat al-Jumhur bemaqahi al-Internet lima' aljins waltajasos wasirqat albareed aleliqtoroni" [Information software to control the relationship between the public and Internet cafés and to prevent access to sex, spying, and stealing emails], *Dar al-Hayat*, June 24, 2007,
 - http://www.daralhayat.com/science_tech/0 6-2007/ltem-20070623-59a6944a-c0a8-10ed-0082-a494ca530035/story.html.
- ⁴¹ Khaled Yacoub Oweis, "Syria expands 'iron censorship' over Internet," *Reuters,* March 13, 2008,
 - http://uk.reuters.com/article/internetNews/idUKL138353620080313?sp=true.
- 42 "Internet cafes closed after midnight," Mareb Press, February 20, 2008, http://marebpress.net/news_details.php?si d=10305.
- ⁴³ Moneer Al-Omari, "Search for Pornographic Material on Rise; Children are most Vulnerable," *Yemen Post*, January 12, 2009, http://www.yemenpost.net/63/Reports/20 084.htm.
- 44 "Egypt demanding data from cyber cafés users: NGO," AFP, August 9, 2008, http://afp.google.com/article/ALeqM5hN_tk tRSmeojLOOn65IVULB4Ij8A.
- ⁴⁵ Moneer Al-Omari, "Search for Pornographic Material on Rise; Children are most Vulnerable," *Yemen Post*, January 12, 2009, http://www.yemenpost.net/63/Reports/20 084.htm.
- ⁴⁶ Oman Telecommunications Company, "Procedures for Internet Cyber Café Pre-Approval," http://www.omantel.net.om/services/busin

ess/internet/preapprovaleng.pdf.