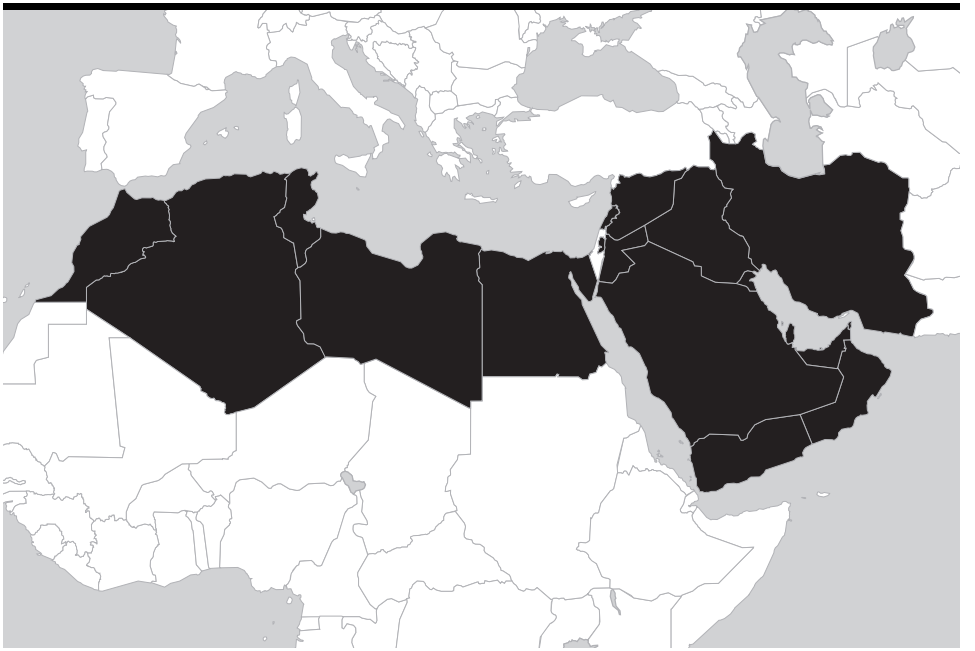
MENA Overview



Introduction

Countries in the Middle East and North Africa continue to invest in information technology infrastructure and media projects as part of their strategies to develop local economies and create employment. Among the major examples is Jordan's plan 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 of the population. It aims to increase employment in the IT sector and to boost the sector's revenues from USD 2.2 billion in 2009 to USD 3 billion by the end of 2011.[1]

In addition to existing regional hubs Dubai Media City and Dubai Internet City, the United Arab Emirates (UAE) 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. Among the partners of the zone are CNN, the BBC, the *Financial Times*, the Thomson Reuters Foundation, and the Thomson Foundation.[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 information and communication technology (ICT) infrastructure that hinders Internet access in the region. WiMAX, for example, was commercially available by the 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 the Internet population. *Arab Media Outlook, 2008–2012* states, "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 of the incumbent telecom companies in North Africa are already in private hands, with the exception of Algérie Télécom, the privatization of which has been postponed because of the global economic crisis.[7] However, experts say telecom liberalization in the Middle East and North Africa still lags behind the rest of the world in terms of cost and efficiency, a matter which does not encourage direct foreign investment.[8]

The Media Environment

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 religion. Such laws have often been used to suppress report-

ing 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, five countries (Egypt, Syria, Iran, Tunisia, and Saudi Arabia) were from the region.[10]

Internet and Media Regulations: The Debate

The last few years have witnessed an increase in debates over media and Internet censorship in the region. Rifts between 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 repressive regulations, which limit freedom of speech online, some governments claim they arrest bloggers and online activists because they exploit 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 Center 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 that 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 Web site offers to facilitate the blocking of Web sites by sending user-submitted URLs of questionable content to 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 anti-censorship 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 religious beliefs or public order.[14]

However, in May 2009 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.[15]

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.[16] These examples and cases illustrate how the fight over access controls is taking different and often more subtle shapes and forms, and also indicate that different players will continue the debate and challenge each other.

Access Control

Access controls in the Middle East and North Africa are multilayered; governments and authorities use first- and second-generation measures to regulate Internet access and online activities. These measures include laws and regulations, technical filtering, physical restrictions, surveillance and monitoring, and harassment and arrests. Among the laws and regulations used to control access in the region are the press and publication laws, penal codes, emergency laws, antiterrorism laws, Internet-specific laws, ISPs' terms and 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.[17] Kuwait's 2006 press law allows the imprisonment of journalists for making references to Islam that are deemed insulting[18] or for articles seen as "against national interests."[19] Oman's 1984 Press and Publication Law authorizes the government to censor publications deemed politically, culturally, or sexually offensive.[20] Syria's 2001 Press Law sets out sweeping controls over publications printed in Syria.[21] Journalists 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.[22] Yemen's 1990 Press and Publications Law subjects publications and broadcast media to broad prohibitions and harsh penalties.[23] The press law in Morocco has been used to suppress outspoken online writers.[24]

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 content on the Internet that "incites hatred" or "harms national interests."[25] Syria's penal code criminalizes spreading news abroad.[26] Though the Bahraini government in May 2008 introduced 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 antiterrorism law.[27]

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 this status to punish individuals deemed threatening. Egypt's emergency law, in force since the declaration of the state of emergency in 1981, grants the government 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.[28] Similarly, Syria uses the ongoing state of emergency (which began in 1963) to arrest media workers.[29]

Morocco uses its antiterrorism 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."[30]

Internet-Specific Laws

Few countries in the region have introduced Internet-specific laws to regulate Internet activities; among them are the UAE 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.[31]

In January 2008, Saudi Arabia implemented 16 articles of a 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 a 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 the maximum punishments.[32]

Terms and Conditions of ISPs

Terms and conditions imposed on users 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 and 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.''[33]

Another example is Yemen, where the terms and conditions set by the ISP TeleYemen (or Y.Net) prohibits ''sending any message which is offensive on moral, religious, communal, or political grounds.'' TeleYemen reserves the right to control access ''and data stored in the Y.Net 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.''[34]

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 Web 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.''[35] Bahrain's Telecommunications Law of 2002 contains penalties for illicit use of the Internet, including the transmission of messages that are offensive to public policy or morals.[36] In Tunisia, the 1998 post and telecommunications law enables the authorities to intercept and check the content of e-mail messages.[37] Electronic surveillance such as filtering of e-mail messages of government opponents has been reported in Tunisia.[38]

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 the 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 cafés were required to collect names and identification numbers of their customers and report this information, together with any suspicious activities, to the police.[39]

Similarly, in March 2008 Jordan began to increase restrictions on the country's Internet cafés. Cameras were installed in Internet cafés to monitor users, and owners were required to register the IP number of the café, their users' personal data, the time of use, and the data of Web sites explored.[40]

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.[41] In Kuwait, Internet café owners also were required to maintain a record of customers' names and identifications, which they must submit to the Ministry of Communications upon request.[42]

Some Internet café operators in Lebanon admit that they use computer surveillance 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.[43] However, there is no evidence that the government orders these measures.

In March 2008, the Syrian authorities ordered Internet café users to provide their names, identification cards, and the times they use the Internet café to café owners, who will consequently present them to the authorities.[44]

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.[45] Some owners use surveillance software to monitor the online activities of their customers and refuse access to clients who access pornography.[46]

In August 2008, Egyptian authorities imposed new monitoring measures by demanding that Internet café clients must provide their names, e-mail addresses, and telephone numbers before they can use the Internet. Once the data are provided, clients will receive a text message on their cell phones and a PIN number that they can use to access the Internet.[47]

In addition to the preceding measures, some countries impose physical restrictions on Internet cafés as part of their monitoring efforts. For example, Yemen[48] and Oman[49] require that computer screens in Internet cafés must be visible to the floor supervisor. No closed rooms or curtains that might obstruct the view of the monitors are allowed.

Technical Filtering

The OpenNet Initiative conducted tests for technical Internet filtering in all the countries in the Middle East and North Africa between 2008 and 2009. Test results prove that the governments and 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, Iran, United Arab Emirates, Syria, Saudi Arabia, Morocco, Libya, and Tunisia have censored Web sites containing content critical of governments and leaders, Web sites that claim human rights violations, and/or Web sites of opposition groups. Mauritania briefly blocked the news Web site Taqadoumy, and Egypt at one 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, Sudan, Tunisia, Gaza, Yemen, and Iran censor pornography, nudity, gay and lesbian content, escort and dating services, and Web sites displaying provocative attire. Also censored by most of these countries are Web sites that 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 can also be used to access blocked content.

Testing by ONI revealed no evidence of technical filtering in Algeria, Iraq, Lebanon, and the West Bank between 2008 and 2009.

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 that 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 Web sites such as YouTube, Facebook, and Amazon, as well as more Web sites affiliated with the Muslim Brotherhood and Kurdish opposition groups. Another example is Tunisia, which added more political and oppositional content as well as other apolitical Web 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. Testing revealed that most of the Arab countries have begun blocking 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. The ONI investigation revealed that the U.S.-based commercial filtering software used by most of the ISPs in the region (e.g., SmartFilter, Websense, and Bluecoat) do not pick up Arabic content as comprehensively as content in other languages.

Increases in filtering are the norm in the Middle East and North Africa, and lifting blocks is the exception. Among the few examples of the unblocking of Web sites are

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 Web sites. Sudan's filtering of gay and lesbian, dating, provocative attire, and health-related Web sites was also more limited compared to previous test results.

Another regional trend toward second-generation controls is that more Arab countries are introducing regulations to make Web publishing subject to press and publication laws, and are requiring local Web sites to register with the authorities before they can go live. In Jordan in September 2007, for example, the country's Legislation Bureau in the Prime Minister's Office issued 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 that it would exercise immediate supervision and censorship.

Another example is Saudi Arabia, which announced in May 2009 plans to enact legislation for newspapers and Web sites that will require Saudi-based 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 through second-generation methods 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 attacks among different religious groups in the region, namely Shiite and Sunni groups, have 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 content from some of these Web sites. Additionally, Israeli, Palestinian, and Lebanese Web sites run by Hezbollah have been targets of attacks, especially during 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.

First- and second-generation access controls are evident throughout the Middle East and North Africa. Censors in the region attempt to control political content using technical filtering, laws and regulations, surveillance and monitoring, physical restrictions, and extralegal 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 various 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 extralegal harassment from security agencies create a climate of fear used to silence online dissidents and conform to second-generation controls found elsewhere in the world.

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 sites and photo and video sharing 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.

Notes

1. Mohammad Ghazal, ''Jordan, UAE Firms in Talks over Free IT Zone,'' *Jordan Times*, May 16, 2009, http://www.jordantimes.com/?news=16742.

2. Keach Hagey, ''Capital Launches Media Zone to Nurture Young Arab Talent,'' *The National*, October 13, 2008, http://www.thenational.ae/article/20081012/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=april2009&file=local_news2009041913642.xml.

4. Arab Advisors Group, ''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,'' April 16, 2009, http://www.arabadvisors.com/Pressers/presser-160409.htm.

5. ChinaCCM, ''2008 Africa—Telecoms, Mobile and Broadband in Northern Region,'' December 2008, http://www.chinaccm.com/4S/4S16/4S1607/news/20081205/111435.asp.

6. PricewaterhouseCoopers, ''Arab Media Outlook, 2008–2012,'' http://www.pwc.com/extweb/pwcpublications.nsf/docid/14D97CB491E2A59B85257334000B8AAB.

7. ChinaCCM, ''2008 Africa—Telecoms, Mobile and Broadband in Northern Region,'' December 2008, http://www.chinaccm.com/4S/4S16/4S1607/news/20081205/111435.asp.

8. Dana Halawi, ''MENA Telecoms Need Liberalization—Hasbani,'' *Daily Star*, April 17, 2009, http://www.dailystar.com.lb/article.asp?edition_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.

10. 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.

11. Arabic Network for Human Rights Information, ''Egypt: New Comic Crimes Written by the State Security: Blogger in Custody, on Charges of Exploitation of the Democratic Climate,'' May 14, 2009, http://anhri.net/en/reports/2009/pr0514-2.shtml.

12. *The Economist*, ''The Limits to Liberalisation,'' May 14, 2009, http://www.economist.com/world/mideast-africa/displaystory.cfm?story_id=13649580.

13. OpenNet Initiative Blog ''Users' Initiative to Block Web Sites,'' October 24, 2008, http://opennet.net/blog/2008/10/users-initiatives-block-web-sites.

14. Arabic Network for Human Rights Information, ''Weekly Update for the Arabic Network for Human Rights Information #192,'' December 28, 2007, http://www.anhri.net/en/newsletter/2008/newsletter1003.shtml.

15. Agence France Presse, ''Cairo Court Rules to Block Porn Sites,'' May 12, 2009, http://newsx.com/story/52677.

16. Lina Ben Mhenni, ''Tunisia: Facebook Case Thrown Out of Court,'' Global Voices Online, November 29, 2008, http://globalvoicesonline.org/2008/11/29/as-usual-the-tunisian-legal-system-has-been-faithful-to-the-values-of-fair-trial/.

17. 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/2446.

18. *BBC News*, ''Country Profile: Kuwait,'' August 10, 2009, http://news.bbc.co.uk/2/hi/middle_east/country_profiles/791053.stm.

19. Reporters Without Borders, ''Kuwait—Annual Report 2007,'' http://www.rsf.org/article.php3?id_article=20767.

20. United Nations Development Program, ''Program on Governance in the Arab Region (UNDP-POGAR): Oman,'' http://www.pogar.org/countries/civil.asp?cid=13.

21. Freedom House, ''Map of Press Freedom 2008,'' 2008, http://www.freedomhouse.org/template.cfm?page=251&year=2008.

22. Joel Campagna, ''Tunisia Report: The Smiling Oppressor,'' Committee to Protect Journalists, September 23, 2008, http://cpj.org/reports/2008/09/tunisia-oppression.php.

23. Yemen News Agency (Saba), Press and Publications Law, http://www.sabanews.net/en/news44000.htm.

24. Reporters Without Borders, ''Appeal Court Overturns Blogger's Conviction,'' September 18, 2008, http://www.rsf.org/article.php3?id_article=28603.

25. Saba News, ''al-Lawzi: ma yunshar fi sahafat alinternet lan yakoun baeedan 'an almusa'lah bimawjeb alqanoon'' [al-Lawzi: Online journalism content will be subject to the penal code], April 1, 2008, http://www.sabanews.net/ar/news150790.htm.

26. Freedom House, ''Map of Press Freedom 2008,'' 2008, http://www.freedomhouse.org/template.cfm?page=251&year=2008.

27. International Federation of Journalists, ''Despite Advances, Journalists Still Face Possible Jail Terms under Prevailing Laws, Warns IFJ,'' June 12, 2008, http://www.ifex.org/en/content/view/full/94435/.

28. Sarah Carr, ''Journalists Challenge Egypt's Exceptional Laws at Seminar,'' *Daily News Egypt*, August 1, 2008, http://dailystaregypt.com/article.aspx?ArticleID=15464.

29. Reporters Without Borders, ''Syria—Annual Report 2007,'' http://www.rsf.org/article.php3?id_article=20777.

30. Human Rights Watch, ''Background: The State of Human Rights in Morocco,'' November 2005, http://hrw.org/reports/2005/morocco1105/4.htm.

31. *Gulf News*, ''UAE Cyber Crimes Law,'' November 2, 2007, http://archive.gulfnews.com/uae/uaessentials/more_stories/10018507.html.

32. David Westley, ''Saudi Tightens Grip on Internet Use,'' *Arabian Business*, January 26, 2008, http://www.arabianbusiness.com/509226-saudi-tightens-grip-on-internet-useoni.

33. Omantel, ''Omantel Terms and Conditions,'' http://www.omantel.net.om/policy/terms.asp.

34. Y.Net, ''Terms and Conditions for Y.Net Service,'' http://www.y.net.ye/support/rules.htm.

35. Reporters Without Borders, ''Internet under Surveillance 2004—Algeria,'' 2004, http://www.rsf.org/spip.php?page=article&id_article=10806.

36. 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.

37. Reporters Without Borders, ''A Textbook Case in Press Censorship for the Past 20 Years,'' November 5, 2007, http://www.rsf.org/article.php3?id_article=24264.

38. Reporters Without Borders, ''Repression Continues as Ben Ali Marks 21st Anniversary as President,'' November 7, 2008, http://www.rsf.org/article.php3?id_article=29208.

39. Fathiya Borowinah, ''*al-Jazaer: Ajhizat alamn tolin al-harb ala magahi alinternet liihbat masharee' khalaya irhabiya naemah*'' [Algeria: Security apparatus declares war on cyber cafes to abort potential

terrorist activities of sleeping cells], *Al-Riyadh*, May 1, 2007, http://www.alriyadh.com/2007/05/01/article246175.html.

40. Arabic Network for Human Rights Information, ''Jordan: New Restrictions on Internet Cafes and Violating Privacy of Users,'' March 11, 2008, http://anhri.net/en/reports/2008/pr0311.shtml.

41. OpenNet Initiative Blog, ''Restriction on Internet Use in the Middle East on the Rise: Internet Cafés in Saudi Must Install Hidden Cameras,'' April 16, 2009, http://opennet.net/blog/2009/04/restriction-internet-use-middle-east-rise-internet-caf%C3%A9s-saudi-must-install-hidden-came.

42. 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.

43. *Dar al-Hayat*, ''*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 e-mails], June 24, 2007.

44. Khaled Yacoub Oweis, ''Syria Expands 'Iron Censorship' over Internet,'' Reuters, March 13, 2008, http://uk.reuters.com/article/internetNews/idUKL138353620080313?sp=true.

45. *Mareb Press*, ''Internet Cafés Closed after Midnight,'' February 20, 2008, http://marebpress.net/news_details.php?sid=10305.

46. Moneer Al-Omari, ''Search for Pornographic Material on Rise; Children Are Most Vulnerable,'' *Yemen Post*, January 12, 2009, http://www.yemenpost.net/63/Reports/20084.htm.

47. Agence France Presse, ''Egypt Demanding Data from Cyber Cafés Users: NGO,'' August 9, 2008, http://afp.google.com/article/ALeqM5hN_tktRSmeojLOOn65lVULB4lj8A.

48. Moneer Al-Omari, ''Search for Pornographic Material on Rise; Children Are Most Vulnerable,'' *Yemen Post*, January 12, 2009, http://www.yemenpost.net/63/Reports/20084.htm.

49. Oman Telecommunications Company, ''Procedures for Internet Cyber Café Pre-Approval,'' http://www.omantel.net.om/services/business/internet/preapprovaleng.pdf.

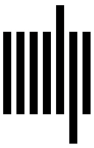
Access Controlled

The Shaping of Power, Rights, and Rule in Cyberspace

Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

Citation:

Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/8551.001.0001
ISBN (electronic): 9780262266031
Publisher: The MIT Press
Published: 2010



The MIT Press

For information about special quantity discounts, please email special_sales@mitpress.mit.edu

This book was set in Stone Serif and Stone Sans on 3B2 by Asco Typesetters, Hong Kong.

Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access controlled : the shaping of power, rights, and rule in cyberspace / edited by Ronald Deibert . . . [et al.] ; foreword by Miklos Haraszti.
p. cm. — (Information revolution and global politics)
Report from the OpenNet Initiative.
Includes bibliographical references and index.
ISBN 978-0-262-01434-2 (hardcover : alk. paper) — ISBN 978-0-262-51435-4 (pbk. : alk. paper)
1. Cyberspace—Government policy. 2. Internet—Government policy. 3. Computers—Access control. 4. Internet—Censorship. I. Deibert, Ronald. II. OpenNet Initiative.
HM851.A254 2010
005.8—dc22 2009049632

10 9 8 7 6 5 4 3 2 1