OpenNet Initiative

Country Study
Internet Filtering in Tunisia, 2005

November 2005

Internet Filtering in Tunisia in 2005: A Country Study

OpenNet Initiative

http://www.opennetinitiative.net/tunisia

Internet Filtering in Tunisia in 2005

1.   EXECUTIVE SUMMARY

  The Tunisian Republic implements an Internet filtering regime that aggressively targets and blocks substantial on-line material on political opposition, human rights, methods of bypassing filtering, and pornography. Tunisia's position as host of the United Nations (UN) World Summit on the Information Society (WSIS) in November 2005 has cast a spotlight on the state's information technology and media policies. In preparations for the WSIS meeting, human rights and media organizations have increased their criticism of Tunisia's widespread censorship practices and Internet controls. For example, the International Freedom of Expression eXchange (IFEX) formed the Tunisia Monitoring Group (TMG), a coalition of 13 organizations, to challenge the state's practices and to urge the UN to pressure Tunisia to make immediate reforms or forfeit the summit.[1]

  To document the extent of Tunisia's Internet content controls, the OpenNet Initiative (ONI) tested 1923 sites from within the state, and found 187 (10%) blocked. Tunisia's filtering efforts are focused and effective. The state employs the SmartFilter software, produced by the U.S. company Secure Computing, to target and prevent access to four types of material in particular: political opposition to the ruling government, sites on human rights in Tunisia, tools that enable users to circumvent these controls, and pages containing pornography or other sexually explicit content.

  The Tunisian state clearly views the Internet as a powerful social and economic force and has invested in telecommunications infrastructure and passed modern telecommunications legislation. Tunisia has deployed the Internet in a way that implements a multi-layered architecture of control. All of the state's Internet Service Providers (ISPs) purchase access from Tunisia's Internet Agency, which performs filtering at the network backbone. This ensures greater consistency of control. In addition, the primary means of going on-line for Tunisians are the "Publinets" – Internet cafés that are required by the state to monitor users' access to prevent them from obtaining prohibited materials.

  Moreover, Tunisia's approach to the Internet comports with the strong limitations the state imposes on other media. Laws criminalizing defamation of public officials or spreading false news push journalists to censor their reporting, and the imprisonment of critics of the government makes plain that these laws have bite. The state also employs a mixture of economic controls, such as directing subsidies and advertising to friendly outlets, and informal pressures, such as violence against critics, to ensure that media stay within prescribed boundaries.

  The World Summit on the Information Society is committed to a vision where "everyone can create, access, utilize and share information and knowledge," where each person has the

---

[1] International Freedom of Expression eXchange (IFEX), *The IFEX Tunisia Monitoring Group*, *at* http://campaigns.ifex.org/tmg/about.html; IFEX, *Tunisia: Freedom of Expression Under Siege*, Feb. 2005, *available at* http://www.ifex.org/download/en/FreedomofExpressionunderSiege.doc.

right "to seek, receive and impart information and ideas through any media."[2] To have the Summit hosted in Tunisia, a state where information is controlled through a mixture of legal, technical, and economic means, belies these goals and highlights the growing contradiction between lofty principles of free expression and communication often associated with the Internet by policymakers and industry, and the reality of censorship and surveillance practices worldwide. As with several other countries the ONI has studied, Tunisia is part of a growing trend whereby software developed by Western corporations is used by repressive regimes to restrict access to information and curb freedom of speech.

2. POLITICAL, TECHNICAL, AND LEGAL CONTEXT IN TUNISIA

A. Sensitive/Controversial Topics for Media Coverage

The most sensitive media topic in Tunisia is criticism of the government. In public, President Zine El Abidine Ben Ali has called on Tunisian journalists to refrain from self-censorship.[3] However, the government does not tolerate criticism and imposes direct or de facto restrictions on coverage of opposition politics.[4] No newspaper opposed constitutional reforms in 2002 that allowed the President to stand for unlimited terms of office.[5] During the most recent presidential and legislative elections in October 2004, the major media paid little attention to opposition candidates while providing President Ben Ali and the ruling party highly favorable and disproportionate coverage.[6]

In March 2004, a group of journalists working for the state-owned daily publications *La Presse* and *Essahafa* sent a letter to the government complaining of pervasive censorship and distortion of their work by editors operating on orders from the state.[7] Restricted items have included coverage of local human rights groups, natural disasters, cases of torture in police custody, an Amnesty International advertisement, and President Ben Ali's postponement of the Arab League Summit in Tunis.[8] One analyst stated, "The government's no-go areas for the media are corruption and human-rights issues. This includes discussion of banned Islamic movements, whose strength is hard to gauge because of a comprehensive government crackdown on their activities throughout the 1990s."[9] The government fears opening the door to

---

[2] World Summit on the Information Society, *Declaration of Principles*, Dec. 12, 2003, *available at* http://www.itu.int/wsis/docs/geneva/official/dop.html.
[3] IFEX, *The IFEX Tunisia Monitoring Group: Media Censorship, at* http://campaigns.ifex.org/tmg/censorship.html.
[4] *See, e.g., Country Profile: Tunisia*, BBC News, Aug. 4, 2005, *at* http://news.bbc.co.uk/1/hi/world/middle_east/country_profiles/791969.stm.
[5] Roland Lank, *Tunisia: Seven Versions of Pravda*, World Press.org, Feb. 18, 2003, *at* http://worldpress.org/Mideast/957.cfm.
[6] Human Rights Watch (HRW), *Human Rights Overview: Tunisia, at* http://hrw.org/english/docs/2005/01/13/tunisi9801.htm (Jan. 13, 2005).
[7] IFEX, *The IFEX Tunisia Monitoring Group: Media Censorship.*
[8] *Id.*
[9] Lank, *Tunisia: Seven Versions of Pravda.*

criticism because of concerns it may embolden its critics.[10] Sensitive news topics, then, appear to include any that might reflect poorly on the government.

B.   Internet Infrastructure and Access

Tunisia's Internet infrastructure is composed of multiple ISPs, with centralized filtering carried out by a government agency that controls the network backbone. In 1996, the Tunisian Ministry of Communications formed the Tunisian Internet Agency (ATI) to take control of Tunisia's Internet backbone and DNS services from the Regional Institute for Computer Sciences and Telecommunications (IRSIT) in Tunis.[11] Tunisia obtains wireline bandwidth from five primary sources:

Provider	Location
France Telecom	France
Teleglobe	America
Telecom Italia	Italy
Flag Telecom	United Kingdom
EUMEDCONNECT	Italy

Figure 1 - Tunisia's Upstream Bandwidth Providers[12]

According to the state, these sources combine for a total of 75.5 Mbps bandwidth.

Tunisia's 12 Internet Service Providers lease their bandwidth from ATI.[13] Of these, seven are state-owned and serve government and educational institutions exclusively, leaving five choices for private access: Planet Tunisie, 3S Global Net, Hexabyte, Tunet and Topnet.[14] Competition among these providers has led them to adopt similar pricing schemes. Each offers subscription-free hourly dial-up access, with the only cost that of the phone call ($1.20 US during work hours and $0.80 during nights and weekends),[15] and pre-paid access starting at $10 US for 15 hours of access.[16] All ISPs also offer broadband through Asymmetric Digital Subscriber Line (ADSL) to home users, with prices starting at $25 US per month for unlimited 128kbps access.[17] Other high-speed solutions, such as frame relay and ISDN connections, are available to businesses and vary by ISP. In September 2004, Planet Tunisie and Monaco Télécom collaborated to form Divona Télécom, the first private company licensed to offer Very

---

[10] *Id.*

[11] Tunisia Online, *Internet in Tunisia – History*, June 25, 2002, *at* http://www.tunisiaonline.com/internet/history.html.

[12] Robtex.com Network Explorer report on Tunisia Backbone, *available at* http://www.robtex.com/netexp/as2609.

[13] Network Startup Resource Center, *Tunisia and the state of the Internet* (e-mail from Lamia Chaffai of ATI to Dolores Lizarzaburu of NSRC), Nov. 14, 2002, *available at* http://www.nsrc.org/db/lookup/report.php?id=1037285984211:488846420&fromISO=TN.

[14] Tunisia Internet Agency, *Internet en Tunisie*, *at* http://www.ati.nat.tn/internet/fsi.htm (French language only).

[15] *See, e.g., Hexabyte's Free Internet FAQ*, *at* http://www.zerodinar.com/faq.php (French language only).

[16] *See, e.g.,* 3S GlobalNet, *Le Global Pack*, *at* http://www.globalnet.tn/html/abonnements/globalpack.html (French language only).

[17] *See, e.g.,* Topnet, *ASDL rates*, *at* http://www.topnet.tn/acces.php?w=adsl-home (French language only).

Small Aperture Terminal (VSAT) satellite services in competition with state-owned Tunisie Télécom.[18] Satellite-based Internet access can be obtained from both Planet Tunisie and Tunet.[19]

Though relatively inexpensive subscription Internet access is available, computers are still expensive for the average Tunisian citizen, and most of Tunisia's estimated 771,000 Internet users gain access from Internet cafés, known as "Publinets."[20] The first of these public access centers emerged in 1998 as the result of a government project that subsidized 50% of the equipment costs of new locations.[21] According to the state, there are now 305 Publinets across Tunisia.[22] Access at a Publinet costs at most $2.00 US per hour, and students, journalists, and the disabled receive a 25% discount.[23] Publinets serve as a low-tech point of control in Tunisia's Internet infrastructure. Publinet owners are required by the state to monitor customer access to prevent access to "banned" content.[24] The cafés implement this mandate through different methods; in some Publinets, all computer monitors are angled so that administrators can observe them, and in others customers are required to present identification to receive access.[25]

The centralized nature of Tunisia's infrastructure makes consistent filtering technologically straightforward. Since all wireline bandwidth passes through ATI's servers and network, ATI can filter all content passing to and from ISPs, educational institutions, and government offices. ONI's research indicates that this point at ATI is where content filtering takes place in Tunisia, and that ATI employs Secure Computing's SmartFilter software for filtering, so that blocking occurs consistently regardless of the ISP used.[26]

C.   Media Ownership and Control

The Tunisian government Web site Tunisia Online (http://www.tunisiaonline.com) touts the government's commitment to freedom of the press, human rights, pluralism, and tolerance.[27] The state promotes the reforms to media regulation that President Ben Ali ushered in with the May 2001 Press Law amendments, which theoretically include the elimination of prison sentences for journalists and of the charge of "defaming public order."[28] The government's media regulation body, the Tunisian External Communication Agency (ATCE),

---

[18] Alcatel, *Divona Télécom Tunisia chooses the Alcatel DVB-RCS satellite solution to develop its high speed Internet service*, Sept. 10, 2004, *at* http://www.home.alcatel.com/vpr/archive.nsf/DateKey/10092004_1uk.

[19] Tunet.tn, *L'accès Internet haut débit par satellite (TUNET VSAT)*, *at* http://www.tunet.tn/?item=solutions&sp=Satellite (French language only).

[20] Agence Tunnisienne d'Internet (ATI), *Internet en Tunisie*, *at* http://www.ati.nat.tn/internet/index.htm (French language only).

[21] Tunisia Online, *The Publinet Project*, *at* http://www.tunisiaonline.com/internet/publinet.html (last updated June 25, 2002).

[22] ATI, *Internet en Tunisie*.

[23] ATI, *Les centres d'accès publics (Publinets)*, *at* http://www.ati.nat.tn/publinets/index.htm (French language only).

[24] IFEX Tunisia Monitoring Group, *Tunisia: Freedom of Expression under Siege* at 24.

[25] Human Rights Watch, *The Internet in the Mideast and North Africa: Free Expression and Censorship*, *at* http://hrw.org/advocacy/internet/mena/tunisia.htm.

[26] *See also* IFEX Tunisia Monitoring Group, *Tunisia: Freedom of Expression under Siege* at 25.

[27] Tunisia Online, *Government*, *at* http://www.tunisiaonline.com/government/index.html.

[28] *Id.*

claims that fewer than 10 percent of newspapers are publicly owned or controlled.[29] ATCE Director General Oussama Romdhani wrote in response to a critical press article that "The majority of Tunisia's 244 newspapers and magazines are essentially private and do express a variety of views."[30] Romdhani added that the government tolerates dissent and even subsidizes and advertises in opposition papers.[31]

The reality is quite different. The Tunisian state continues to control and systemically suppress media to such an extent that the country earned direct criticism in 2004 from U.S. President George W. Bush, despite Tunisia's cooperation with the U.S. in counterterrorism efforts.[32] The state controls the print and broadcast media, and the few independent outlets and journalists that exist face harassment or imprisonment.[33] The government's claim to have eliminated prison sentences for journalists appears to be both a mistranslation and a mischaracterization of the Press Law, which retains prison sentences under Articles 49, 51, and 52, among others.[34] The law continues to impose stiff fines and prison sentences for journalists who defame public officials or disturb the public order.[35] A number of high-profile events in 2005 highlighted the government's practice of censorship through imprisonment of its critics, in particular the imprisonment of attorney Mohamed Abbou and the death of Tunezine editor Zouhair Yahyaoui, who had been released from prison in 2003 after serving most of a two-year sentence.[36]

With respect to media ownership and control, a Worldpress.org article characterizes Tunisia's media policies as "Stalinist."[37] The state controls the country's three television stations (two network and one satellite) and seven radio stations, and owns several major newspapers in conjunction with the ruling RDC party.[38] The main Arabic-language dailies *Al-Sabah* and *Al-Shurouq* are privately-owned; while there are some opposition newspapers, the ATCE keeps these "on a leash" through control of advertising dollars and subsidies, and consequently they do not challenge the government.[39] "As a result there are two styles of journalism in Tunisia: anodyne daily news reports of government actions, and a flood of tabloid-style crime, entertainment, and gossip news."[40]

---

[29] IFEX, *The IFEX Tunisia Monitoring Group: Media Censorship*.
[30] Letter of Oussama Romdhani to World Press.org, *available at* http://www.worldpress.org/Mideast/971.cfm#down.
[31] *Id.*
[32] HRW, *Human Rights Overview: Tunisia*.
[33] *Id.*
[34] Art. 51, Code de la Presse (Tunisia). The translated text indicates that the 2001 amendments are included. Another explanation for this discrepancy might be that the government transferred certain sections of the Press Law to the Penal Code, as explained in the Tunisian Human Rights League (LTDH) report "Media Under Watch: Tunisia-May 2004."
[35] *Id.*
[36] Additional examples of journalists and opposition leaders imprisoned in Tunisia can be found at IFEX, *Prisoners of Opinion*, *at* http://campaigns.ifex.org/tmg/prisoners.html.
[37] Lank, *Tunisia: Seven Versions of Pravda*.
[38] *Id.*
[39] *Id.*; IFEX, *The IFEX Tunisia Monitoring Group: Media Censorship*.
[40] *Id.*

The Tunisian League for the Defense of Human Rights (LTDH) nonetheless reported a number of positive developments in press freedom in 2003, including the regular publication of the opposition periodicals *El Maoukef* (of the Progressive Democratic Party), *Ettarik El Jedid* (of the Ettajdid movement), and *Al Ouihda* (of the Popular Unity Party).[41] In addition, the government announced that it would open up television networks to limited private investment, ending decades of state monopoly.[42] LTDH also noted the 2003 release on parole of Zouhair Yahyaoui.

D. General Media Regulation

The country's Press Law, most recently amended in 2001, makes defamation of a public official a criminal offense, subjecting a reporter to potential penalties of a minimum of one year in prison and a fine of 120 dinars, or approximately US$90.[43] Publication of false reports that "upset public order" can result in up to three years in prison and a fine of about US$1,500.[44] The laws are not idle threats. In June 2002, the government imposed a two-year prison sentence on Zouhair Yahiaoui, the editor of www.tunezine.com, a satirical Webzine critical of President Zine el-Abidine Ben Ali.[45] In March 2005, a Tunisian court sentenced attorney Mohamed Abbou to three and a half years in prison for publishing an on-line article on the Tunisnews website (http://www.tunisnews.net/) in August 2004, which compared Tunisia's torture of political prisoners to the U.S. abuse of Iraqi prisoners at Abu Ghraib prison.[46] Authorities charged the lawyer under both the Press and Penal Codes with "publishing false reports inclined to disturb public order," "insult to the judiciary," "inciting the population to break the country's laws," and "publishing articles inclined to disturb public order."[47] Some observers noted that Abbou was only arrested after he published a second article in February 2005 that criticized President Ben Ali for inviting Israel Prime Minister Ariel Sharon to the WSIS.[48] A Tunisian court affirmed Abbou's sentence on June 10.[49] (Perhaps not surprisingly, the Tunisnews site currently displays a scrolling notice in French stating that the site is inaccessible in Tunisia.) In May 2000, unidentified gunmen shot and wounded journalist Riadh Ben Fadhel shortly after he had written a piece in *Le Monde* criticizing the Tunisian

---

[41] Tunisian Human Rights League (LTDH), *Media Under Watch: Tunisia-May 2004*. The Lank article *Tunisia: Seven Versions of Pravda* refers to the first two publications as *Al-Tariq al-Jadid* (The New Way) and *Al-Mawkif* (The Stance).
[42] *Id.*
[43] Art. 51, Code de la Presse (Tunisia) (ONI translation).
[44] *Id.*
[45] Human Rights Watch, *Human Rights Overview: Tunisia.*
[46] Reporters Sans Frontières (RSF) / IFEX, *Lawyer sentenced to prison for posting false news on the Internet*, May 4, 2005, *at* http://www.ifex.org/en/content/view/full/66390.
[47] RSF/IFEX, *Lawyer arrested for posting article online*, Mar. 4, 2005, *at* http://www.ifex.org/en/content/view/full/65094/.
[48] *Id.*
[49] RSF/IFEX, *Lawyer's prison sentence confirmed at new "sham" hearing*, June 13, 2005, *at* http://www.ifex.org/en/content/view/full/67310/.

government.[50] International human rights organizations contended that the shooting was the government's response to the article.[51]

E.   Internet Access Regulation

The primary mode of Internet access for individuals who are not students, researchers, or government employees is the Publinet, of which there are about 305 in Tunisia.[52] Access to Publinets is strictly controlled. Both the Ministry of Telecommunications and the Ministry of the Interior have responsibility for controlling on-line content through the use of Internet filtering software. Publinet owners are expected to report on activities within their shops, and have the right to access anything saved to disk by their customers. They also have the right to demand an individual's national identity card, thus linking on-line activities and saved documents with a user's identity.[53]

ONI, in collaboration with IFEX, tested filtering in Tunisia, and found the consistent use of the SmartFilter content filtering package from Secure Computing.[54] ONI concludes that filtering occurs at the ATI-owned gateway, through which all Tunisian ISPs, public or private, must go to access the wider Internet.[55] ISPs that connect users by satellite can bypass the central gateway, and users may be able to obtain unfiltered access by using a personal account with an ISP that does not rely on the ATI-owned gateway.[56] Since virtually all Internet traffic passes through the state-controlled gateway, government control or ownership of ISPs or access points is not necessary for filtering to occur.

F.   Internet Content Regulation

The SmartFilter software can block pre-defined categories of on-line material that administrators can toggle on and off, but it also allows them to list and block individual Web sites that are not categorized. Tunisia appears to block at least four SmartFilter categories: Anonymizers, Nudity, Pornography, and Sexual Materials. In addition, a large number of political, news, and human rights Web sites have been blocked.[57]

Moreover, Tunisian content filtering is done secretly. When users attempt to access a blocked page, they are not informed that the page is filtered, but instead merely receive a standard error message, as though the attempt failed due to technical reasons such as network

---

[50] IFEX, *The IFEX Tunisia Monitoring Group: Media Censorship*.
[51] *Id.*
[52] Central Intelligence Agency (CIA), *The World Factbook: Tunisia*, *at*
http://www.cia.gov/cia/publications/factbook/geos/ts.html (last updated Aug. 9, 2005).
[53] IFEX, *Tunisia: Freedom of Expression Under Siege*.
[54] For a list of sites found blocked in Tunisia by IFEX, *see* The IFEX Tunisia Monitoring Group, *Internet Blocking*, *at*
http://campaigns.ifex.org/tmg/blocking.html.
[55] Internet Censorship Explorer, *Tunisia: Internet Filtering*, *at* http://ice.citizenlab.org/?p=115 (June 7, 2005).
[56] IFEX, *Tunisia: Freedom of Expression Under Siege*.
[57] Russell Southwood, *WSIS Host Tunisia Guilty of Denying Access to Information by Filtering Internet*, Balancing Act, June 6, 2005, *at* http://allafrica.com/stories/200506061286.html.

errors.[58] This error message misrepresents why the user was unable to access the prohibited page, claiming that the requested page could not be found when, in fact, it was actually blocked by the filtering system.[59] This falsification stands in contrast to the practices of other states that filter using the SmartFilter software, as ONI has documented in previous country studies.[60] SmartFilter offers filtering states the option to display a "block page" that notifies a user that he or she has been prevented from accessing a Web site; employing this option makes a filtering system more transparent.[61]

An informal, less subtle method of content regulation occurs when authorities raid Internet cafés and arrest those who are accessing prohibited sites. In July 2004, a Tunisian appeals court affirmed prison sentences of two to 26 years for the "Zarzis seven," a group of young men seized by police in a raid on a Zarzis café where the men allegedly were viewing terrorist Web sites.[62] According to international monitoring groups who observed the trial, the state tortured the defendants into confessing and charged them with unlikely offenses such as conspiring to bring a bazooka into the country.[63]

3. TESTING METHODOLOGY

A. Methods

ONI performs technical testing across multiple levels of access at multiple time intervals. The team analyzes results within the contextual framework of the target state's filtering technology and regulations. To obtain meaningful, accurate results we:

- generate lists of domain names and URLs that have been or are likely to be blocked;
- enumerate ISPs and national routing topography;
- determine the type, location, and behavior of the filtering technology;
- deploy network interrogation and enumeration software at multiple access points; and
- conduct a thorough statistical analysis of results.

Determining which URLs to test is a vital component of our research, as it reveals the filtering system's technical capacity and content areas subject to blocking. ONI employs three types of lists:

---

[58] Internet Censorship Explorer, *Tunisia: Internet Filtering.*
[59] *See* Appendix 5 for a copy of Tunisia's block page.
[60] *See, e.g.,* OpenNet Initiative, *Internet Filtering in Saudi Arabia in 2004*, *at* http://www.opennetinitiative.net/studies/saudi/; OpenNet Initiative, *Internet Filtering in Iran in 2004-2005*, *at* http://www.opennetinitiative.net/studies/iran/.
[61] *See, e.g.,* Secure Computing, *SmartFilter 4.1 Features and Benefits*, *at* http://www.securecomputing.com/index.cfm?skey=1440 (discussing the "Graphical Block/Warn Pages" feature).
[62] IFEX, *Index on Censorship: Clampdown on the Internet Continues in Tunisia*, July 2004, *at* http://www.ifex.org/en/content/view/full/61061/.
[63] *Id.*

1. a list of "high impact" sites reported to be blocked or likely to be blocked in the state of concern due to their content (for example, political opposition);

2. a "global list" containing a control list of manually categorized Web sites reflecting a range of Internet content (for example, news and hacking sites); ONI tested both the global list it has employed in prior countries studies and a new, updated global list in Tunisia; and

3. a "SmartFilter" list of sites categorized by Secure Computing's SmartFilter content filtering software that allows ONI to determine which of the content categories used by the product are blocked in Tunisia.

To explore Internet filtering, we deploy network interrogation devices and applications, which perform the censorship enumeration, at various Internet access levels. These tools download the ONI testing lists and check whether specific URLs and domains are accessible from that point on the network. Interrogation devices are designed to run inside a state (i.e., behind its firewall) to perform specific, sensitive functions with varying degrees of stealth. Similarly, ONI distributes interrogation applications to trusted volunteers who run the software inside the state. For testing, ONI obtains network access at multiple levels through:

- Proxy servers,
- Long distance dial-up,
- Distributed applications, and
- Dedicated servers.

During initial testing, we use remote computers located in countries that filter. These remote computers are located behind the state's firewalls yet allow access to clients connecting from the wider Internet. We attempt to access the URL and domain name lists through these computers to reveal what content is filtered, and how consistently it is blocked. ONI also tests these lists from control locations in non-filtered states. The testing system flags all URLs and domains that are accessible from the control location, but inaccessible from ones inside the target state, as potentially blocked.

B. Results Analysis

We carefully analyze the data obtained from testing to document the nature of filtered content, to explore the technical capabilities of the target state, and to determine areas that require in-depth study during internal testing. In particular, ONI examines the response received over HTTP when attempting to access filtered content. As discussed, when content is filtered, users often receive a "block page" – a Web page with text indicating that the requested

content cannot be accessed.[64] In other cases, filtering can be less obvious or transparent, appearing to be network errors, redirections, or lengthy timeouts rather than deliberate blocking. We analyze HTTP headers – text sent from the Web server to the browser – to derive information about both the server and the requested page. This information is generally hidden from the end user. However, these headers indicate whether content was successfully accessed or was inaccessible. If an error occurs, the HTTP protocol returns codes that indicate the type of error in the header. Thus, by analyzing the headers captured during testing, we can distinguish between errors caused by Internet filtering and more mundane, unintentional network connection errors.

We classify results in one of four categories:

- URL is accessible both through the local connection and the remote computer (not filtered);
- URL is accessible through the local connection but inaccessible through the remote computer, which returned a different HTTP response code (possibly filtered);
- URL is accessible through the local connection but inaccessible through the remote computer due to a network connection error (possibly filtered, but not definitive); or
- URL is accessible through the local connection but inaccessible through the remote computer; the remote computer returns a block page (filtered).

If a URL is inaccessible through both the local connection and the remote computer, we consider it "dead" and remove it from the results.

The ONI team analyzes blocked, unblocked, and uncertain URLs both at an aggregate level (to estimate the overall level of filtering) and at a category level (to indicate what types of content the state seeks to control). We publish country studies that provide background on a state's political and legal system, lists of tested sites, and analysis of results to reveal and analyze what information a state blocks and how it does so. We note, however, that our results and analysis capture a "snapshot" of a state's filtering system for a specific point or period of time; governments can and do alter the content they block dynamically.

---

[64] *See* Internet Censorship Explorer, *Blockpage.com*, *at* http://www.blockpage.com/gallery/ (defining a block page and providing examples).

C.   Methods Specific to Tunisia

To test Tunisia's Internet filtering system, an ONI volunteer checked four lists of Web sites from inside the state.[65] The volunteer employed ONI's specially-developed testing software application. We conducted tests from an access point on the 3S GlobalNet ISP network. Filtering in Tunisia is generally consistent since it is performed at the network backbone, and not at the ISP. Thus, we believe our results are representative of a Tunisian Internet user's experience.

D. Topics Tested

We tested topics on subjects known to be sensitive to the Tunisian state. These included sites on political opposition movements and figures, circumvention tools such as anonymizer pages, human rights, freedom of expression, religious conversion of Muslims, news, and minority ethnic groups.

4.   RESULTS AND ANALYSIS

A. Summary

In total, ONI tested 1923 URLs in Tunisia, and found 187 blocked (10%). While this level of overall censorship is moderate, aggregate numbers do not fully reveal the focused nature of Tunisia's filtering regime. The state prevents access to the majority – in some cases, nearly all – of sites on topics such as anonymizers and circumvention tools, political opposition, human rights criticism of Tunisia's practices, and pornography. Tunisia's filtering system is concentrated and quite effective.

B. Standard Global List Results

Our standard global list testing found concentrated efforts to block pornography and sites that allow users to circumvent filtering. The list checks 770 sites in 31 categories; 72 sites were filtered in Tunisia (9.4%). Tunisia blocked 36 of 38 pornographic Web sites checked (95%); this effectiveness is characteristic of states that employ commercial filtering software.[66] The state also prevented access to 87% of anonymizer Web sites (20 of 23 tested). Anonymizers allow Internet users to browse the Web without being impeded by filtering or monitored by the ISP or state security services. They are an important "loop hole" in a filtering regime, and many states that filter attempt to close it by blocking such sites.   ONI's results also show some blocking of sites related to filtering itself (2 of 9 tested, 22%).

We detected a lesser degree of filtering for sites featuring humor (3 of 18 tested, 17%), provocative attire (2 of 17, 12%), and gay / lesbian / bisexual issues (4 of 38, 11%). Sites in these

---

[65] ONI expresses its gratitude to this person, who remains anonymous as a safety precaution.
[66] *See, e.g.,* OpenNet Initiative, *Internet Filtering in Saudi Arabia in 2004* (documenting use of SmartFilter to block access to nearly all pornographic material).

categories are often filtered due to overblocking when a state attempts to prevent access to pornographic material; this blocking can also indicate a desire to target potentially offensive content that is not strictly pornography. We found one fanatical religious site blocked of 9 tested (11%). The chart below includes results for all content categories on the standard global list for which Tunisia filtered more than 10% of sites tested.

Standard Global List Results
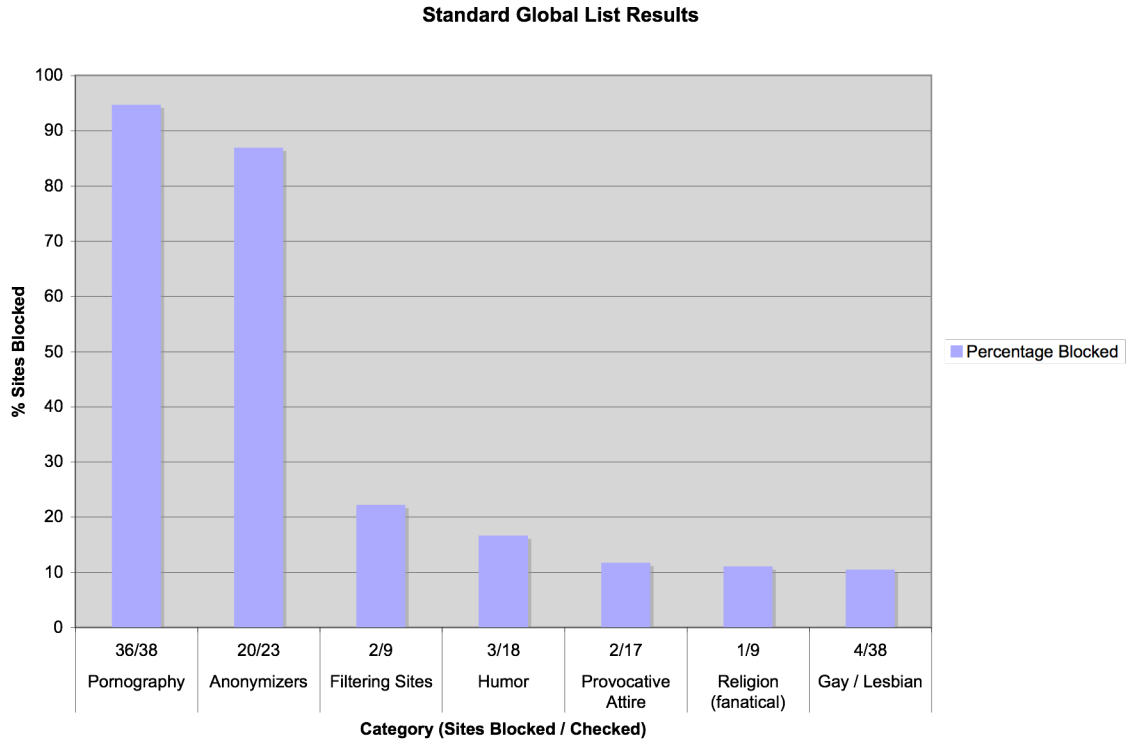
Figure 2 - Standard Global List Filtering (Categories with 10% or more blocked)

C.   New Global List Results

ONI's updated global list, which includes a basket of well-known Internet sites in 27 categories, tests 459 URLs. Tunisia filtered 42 of these sites (9.2%). Of the 27 categories of sites we tested, Tunisia blocked at least one site in 12. As noted, Tunisia appears strongly concerned about preventing users from bypassing the state's ability to block and monitor on-line content. Of the 13 anonymizer sites ONI checked, Tunisia blocked 12 (92%). The state also blocked one-quarter of language translation sites tested (4 of 17, 24%). Like anonymizers, translation sites can permit users to reach blocked content. A user who requests that such a site translate a filtered page can often read the prohibited content since it is the translation site, not the user, that accesses the blocked content.

ONI also found filtering of some gay / lesbian / bisexual sites (3 blocked of 10 tested, 30%), provocative attire sites (4 of 14 blocked, 29%), violent sites (1 of 4, 25%), dating sites (4 of 29, 14%), and pages related to hacking (1 of 8, 13%). There was limited filtering of medical sites (3 of 27, 11%), religious conversion sites (3 of 28, 11%), sites classified as related to terrorism by the U.S. State Department (4 of 39, 10%), and human rights pages (1 of 10, 10%). The graph below displays blocking in categories that had 10% or more of tested sites filtered.
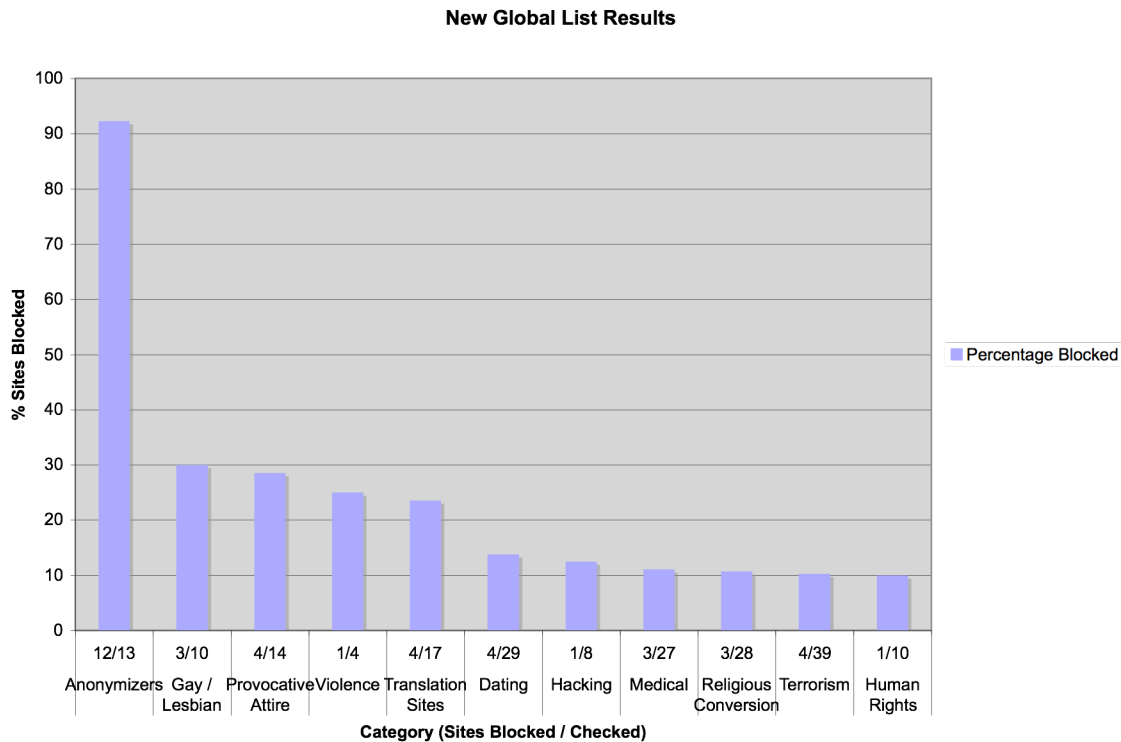
Figure 3 - New Global List Filtering (Categories with 10% or more blocked)

D. Tunisia High-Impact List Results

       The high-impact list, which contains sites on topics known to be sensitive to the Tunisian state from ONI's contextual research, includes 110 URLs. Tunisia blocked 39 of these pages (35%). We found that Tunisia blocks significant content that is critical of, or opposed to, the current government and its practices in areas such as human rights, treatment of political prisoners, and conduct regarding opposition political movements.

       The high-impact list comprises sites in 16 different topic areas. The chart below summarizes our testing results for each category:

Category	Sites Blocked / Tested (% Blocked)
News – Opposition-Focused	4 / 4 (100%)
Music	1 / 1 (100%)
SmartFilter Misclassified[67]	9 / 13 (69%)
Islamist	1 / 2 (50%)
Political Opposition	7 / 14 (50%)
Human Rights	11 / 29 (38%)
News	6 / 25 (24%)
Religious Conversion	0 / 7
Domestic Ethnic Groups	0 / 5
Algeria	0 / 4
Pro-Constitutional Reform	0 / 1
Religion (Islam)	0 / 1
History	0 / 1
Foreign Guerrilla Groups	0 / 1
Weather	0 / 1
Sensitive Keyword in URL[68]	0 / 1

Figure 4 - High-Impact Results by Category

       We note that sites could, in some cases, fall into more than one category – for example, opposition political sites often criticize the Tunisian state's human rights record. However, we attempted to classify sites based on their primary purpose or focus.

       Tunisia's focus is clear: the state concentrates on preventing access to sites that provide information opposed to the current government politically or critical of its practices. The high rate of blocking of news sites with a perspective that is politically counter to the government and of opposition sites reinforces this finding. Blocked political sites include those of the

---

[67] ONI has identified certain sites that are improperly classified by the SmartFilter software; we test these sites to identify that a state is, in fact, using the SmartFilter software to block access to certain material.
[68] This site did not contain sensitive material, but had a keyword in its URL common to sites with sensitive material. We checked this site to test for overblocking by Tunisia.

unauthorized Congrés Pour la République (CPR) party (at several URLs), the banned newspaper of the Tunisian Workers' Communist Party, and the former site of the Movement of Democratic Socialists party. Filtered news sites with an opposition slant include the Réveil Tunisien page and the Perspectives Tunisiennes site, which is "for a democratic, modern, and prosperous Tunisia."[69] Similarly, Tunisia prevents access to the URLs for the Tunisian League for the Defense of Human Rights, the French page for Reporters Sans Frontières, the General Tunisian Student Union, and the human rights group Vérité-Action. The state blocks the site of the banned Islamist group al-Nahdha.

Interestingly, Tunisia did not block any of the sites we tested that are focused on converting adherents of Islam to other religions (primarily Christian denominations), or sites on domestic ethnic groups such as the Berbers. ONI has previously found filtering of these religious conversion sites to be common in states with a population that has a Muslim majority.[70]

Our high-impact testing demonstrates that Tunisia uses the SmartFilter software to block sites on political opposition, criticism of the state's human rights practices, independent news (particularly that aligned with dissident political groups), and non-governmental organizations focused on human rights.

E.   SmartFilter List Results

The SmartFilter content blocking software allows a filtering state to select one or more categories of material that it wishes to prevent users from accessing, such as "Pornography" and "Phishing."[71] To elucidate which categories a filtering state chooses to block, ONI tests a list of sites known to fall into specific categories. This allows us to determine with a high degree of confidence which SmartFilter categories a state has activated; if a site is classified under one of the active categories, it will be blocked in that state. The list checks 587 sites in 63 categories. Tunisia blocked 34 (5.8%).

ONI's testing results indicate that Tunisia uses the SmartFilter content blocking software to target two categories of material: pornographic or sexually explicit sites, and anonymizer sites that allow users to bypass the state's filtering. The state filtered all 15 sites categorized as Nudity (100%) and all 3 categorized as pornography (100%). In addition, Tunisia blocked 2 of 6 sites classified as Sexual Materials (33%), though only 1 of 14 grouped as Provocative Attire (7%). We found that Tunisia blocked 5 of 6 sites (83%) in the category of Anonymizers, along with 1 of 4 Anonymizing Utilities sites (25%). These results accord with our testing of anonymizers in ONI's new global list (which found 92% of sites tested filtered) and standard global list (87%).

---

[69] *Available at* http://www.perspectivestunisiennes.net/ (ONI translation).
[70] See, e.g., OpenNet Initiative, *Internet Filtering in Saudi Arabia in 2004*; OpenNet Initiative, *Internet Filtering in the United Arab Emirates in 2004-2005: A Country Study*, *at* http://www.opennetinitiative.net/studies/uae/.
[71] *See* Secure Computing, *Control List*, *at* http://www.securecomputing.com/index.cfm?skey=86#categories (listing categories SmartFilter uses to classify sites).

For other SmartFilter content categories, our testing found only two with more than 10% of sites blocked: Extreme (1 site of 6 tested, 17%) and Violence (1 of 4, 25%). Thus, out of 63 SmartFilter categories checked, 7 had more than 10% of tested sites blocked, and 13 had any sites filtered. Accordingly, we conclude that Tunisia has chosen to activate at least the SmartFilter categories Anonymizers, Nudity, Pornography, and Sexual Materials, thereby blocking pages classified by Secure Computing as falling under those labels. This type of content is relatively global in nature – many states seek to block pornographic pages – and hence using a commercial software product to classify and filter such material is efficient and effective. In contrast, Tunisia must identify sites germane to its specific concerns, such as political opposition, and block them manually.

The chart below lists all SmartFilter categories where ONI's testing found blocking of more than 10% of sites checked.
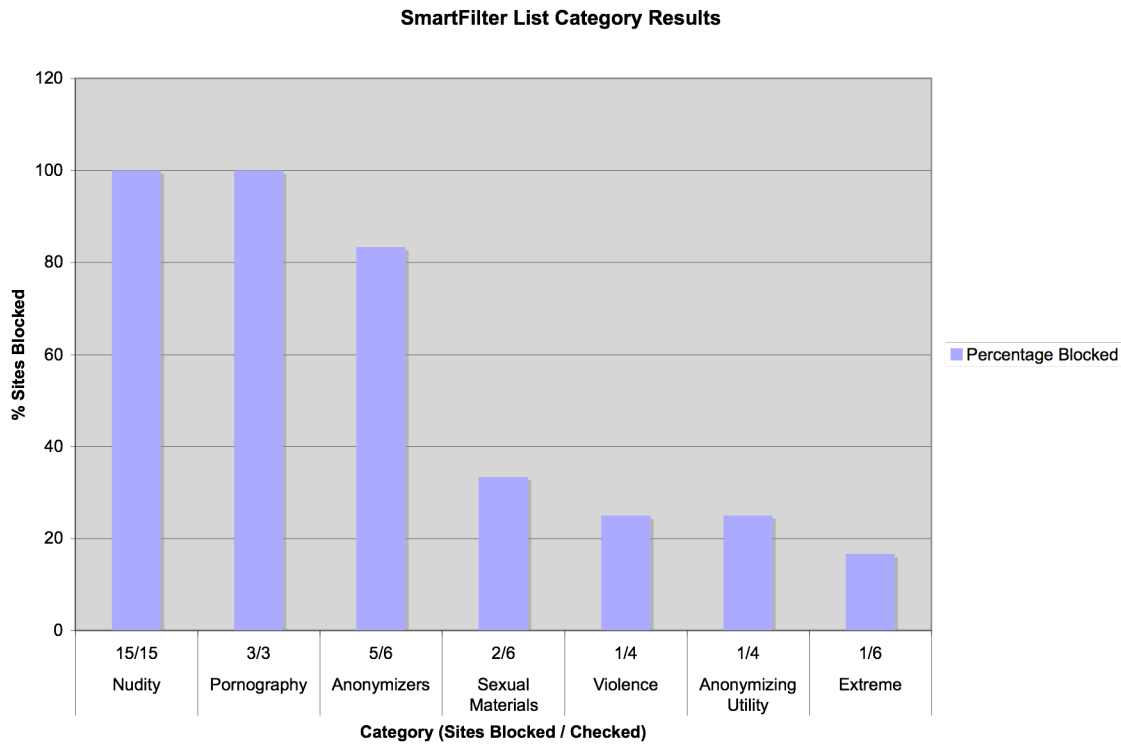
Figure 5 - SmartFilter List Results (Categories with 10% or more sites blocked)

5. CONCLUSION

        In Tunisia, citizens may be theoretically free to receive and share information, but they are practically prevented from doing so on a number of vital topics by a state that combines sophisticated American technology, harsh laws, and informal pressures to limit access. Tunisia focuses its efforts on four areas: political opposition, criticism of the government's human rights record, methods of circumventing filtering, and pornography. Unlike other states employing filtering software that ONI has studied, Tunisia actively disguises its blocking by presenting users with a fake error page instead of the "block page" offered by SmartFilter. This decreases the transparency of Tunisia's filtering and prevents users from understanding the boundaries of blocked content. In sum, Tunisia maintains a focused, effective system of Internet control that blends multiple methods to make some on-line material simply unavailable from within its borders. The stark contrast between Tunisia's censorship regime and the lofty goals of the World Summit on the Information Society call into question the United Nations decision to hold the summit in Tunis.

Standard Global List Testing Results

Category	Number of Sites Tested	Number of Sites Blocked in In-Country Testing
Alcohol	22	0
Anonymizers	23	20 (87%)
Blogging Domains	18	0
Drugs	28	0
E-mail	21	0
Encryption	10	0
Entertainment	27	0
Famous Bloggers	21	0
Filtering Sites	9	2 (22%)
Free Web Space	11	0
Gambling	26	0
Gay / Lesbian / Bisexual / Transgender / Queer Issues	38	4 (11%)
Government	55	0
Groups (including Usenet)	18	0
Hacking	22	0
Hate Speech	23	1 (4%)
Human Rights	28	0
Humor	18	3 (17%)
Major Events	30	0
Miscellaneous	13	0
News Outlets	36	0
Porn	38	36 (95%)
Provocative Attire	17	2 (12%)
Religion (fanatical)	9	1 (11%)
Religion (normal)	52	2 (4%)
Search Engines	27	0
Sex Education	30	0
Translation Sites	13	0
Universities	32	0
Weapons / Violence	28	0
Women's Rights	27	1 (4%)
Total	**770**	**72 (9.3%)**

New Global List Testing Results

Category	Number of Sites Tested	Number of Sites Blocked in In-Country Testing
Alcohol / Drugs / Tobacco	5	0
Anonymizers	13	12 (92%)
Blogging Domains	15	0
Dating	29	4 (14%)
E-mail	2	0
Environment	29	0
Filtering Sites / Free Speech Organizations	16	0
Free Web Space	29	1 (3%)
Gambling	21	0
Gay / Lesbian / Bisexual / Transgender / Queer Issues	10	3 (30%)
Groups (including Usenet)	13	0
Hacking	8	1 (13%)
Hate Speech / Extremist	1	0
Human Rights	10	1 (10%)
Intergovernmental / Funding & Development Agencies	29	0
Medical	27	3 (11%)
Miscellaneous	2	0
News Outlets	1	0
P2P	30	0
Provocative Attire	14	4 (29%)
Religion (Traditional and Non-Traditional)	5	0
Religious Conversion	28	3 (11%)
Search Engines	3	0
Sex Education	12	1 (8%)
Terrorism (U.S. State Department List)	39	4 (10%)
Translation Sites	17	4 (24%)
Violence	4	1 (25%)
VoIP	30	0
Women's Rights	17	0
Total	**459**	**42 (9.2%)**

<u>APPENDIX 3</u>

SmartFilter List Testing Results

Category	Number of Sites Tested	Number of Sites Blocked in In-Country Testing
Alcohol	10	0
Anonymizers	6	5 (83%)
Anonymizing Utilities	4	1 (25%)
Art / Culture / Heritage	13	0
Auction	11	0
Business	14	0
Chat	12	0
Computing / Internet	13	0
Consumer Information	15	0
Criminal Skills	11	0
Dating / Personals	12	0
Drugs	12	0
Educational / Reference	11	0
Entertainment / Recreation / Hobbies	15	0
Extreme	6	1 (17%)
For Kids	1	0
Forum / Bulletin Boards	14	0
Gambling	11	0
Games	14	0
General News	3	0
Government / Military	10	0
Hacking	3	0
Hate Speech	5	0
Health	11	0
History	1	0
Humor	12	0
Instant Messaging	5	0
Internet Radio / TV	13	0
Job Search	17	0
Malicious Sites	1	0
Media Downloads	12	1 (8%)
Mobile Phone	7	0

Non-Profit Organizations / Advocacy Groups	8	0
Not Categorized	17	1 (6%)
Nudity	15	15 (100%)
P2P / Personal Network Storage	4	0
Personal Pages	12	1 (8%)
Politics / Opinion	10	0
Pornography	3	3 (100%)
Portal Sites	13	0
Profanity	14	0
Provocative Attire	14	1 (7%)
Religion and Ideology	13	0
Remote Access	1	0
Resource Sharing	4	0
School Cheating Information	4	0
Search Engines	13	0
Sexual Materials	6	2 (33%)
Shareware / Freeware	8	0
Shopping / Merchandise	13	0
Sports	15	0
Spyware	1	0
Stock Trading	16	0
Streaming Media	10	0
Tasteless / Gross	2	0
Tobacco	14	0
Travel	14	1 (7%)
Usenet News	7	0
Violence	4	1 (25%)
Weapons	14	1 (7%)
Web Ads	10	0
Web Phone	3	0
Total	**587**	**34 (5.8%)**

<u>APPENDIX 4</u>

Tunisia Background

A. <u>Demographics</u>

      The Tunisian Republic is a country of 10 million people and 24 provinces located in Northern Africa on the Mediterranean Sea, between Algeria and Libya.[72] A former French colony, Tunisia declared independence in 1956 and has developed as a moderate Islamic state where fundamentalist Islam is repressed.[73] Although 98 percent of the population is Muslim, for example, the Islamic fundamentalist party Al Nahda is outlawed.[74] Western nations have been moderately critical of Tunisia's human rights record, but the United States has praised the government of President Zine el-Abidine Ben Ali for its support of counter-terrorism efforts, and the European Union maintains an association agreement with Tunisia.[75] The country has a poverty rate of 7.5 percent, unemployment of 13.8 percent, and a literacy rate of 74 percent, with a significantly higher rate among men than women.

B. <u>Economy</u>

      Tunisia's main industries include petroleum, mining and tourism.[76]

C. <u>Politics</u>

      Tunisia is an ostensibly democratic republic where the ruling Constitutional Democratic Assembly Party (RDC) holds a virtual lock on power and opposition parties are weak.[77] The president is elected for five-year terms and appoints the prime minister. The legislative branch is unicameral, consisting of a Chamber of Deputies with 189 seats, 152 of which are occupied by the RDC.[78] The voting age is 20 and suffrage is universal.[79] President Ben Ali, who has been in office since 1987, amended the Constitution in 2002 to remove the three-term limit for presidents and then won re-election by 94.5 percent in October 2004. Human rights groups widely criticized the election, noting that President Ben Ali received the endorsements of two of his opponents.[80]

---

[72] CIA, *The World Factbook: Tunisia*.
[73] *Id.*
[74] *Id.*
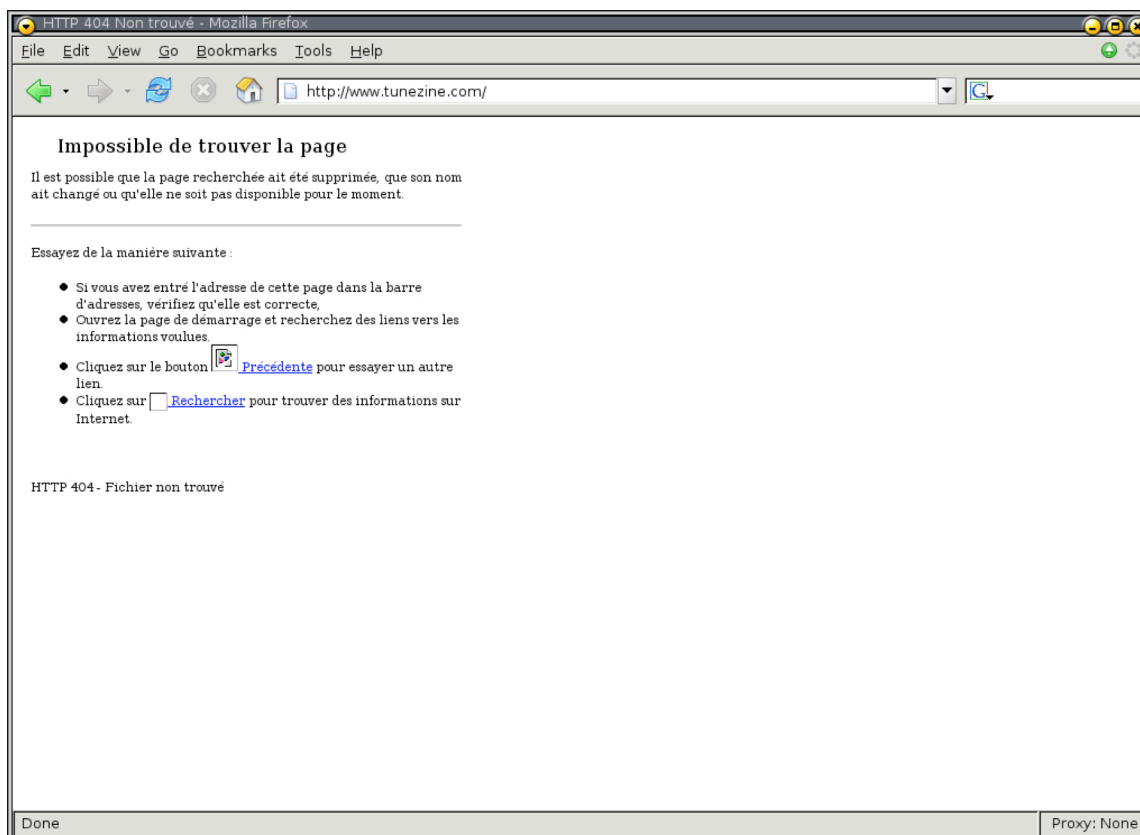[75] HRW, *Human Rights Overview: Tunisia*.
[76] CIA, *The World Factbook: Tunisia*.
[77] *Id.*; HRW, *Human Rights Overview: Tunisia*.
[78] CIA, *The World Factbook: Tunisia*.
[79] *Id.*
[80] HRW, *Human Rights Overview: Tunisia*.

<u>A</u><small>PPENDIX</small> 5

Copy of Falsified Block Page from Tunisia

ONI obtained this copy of a block page from its testing in Tunisia when we attempted to access the filtered site www.tunezine.com. (The block page is generated by a NetApp NetCache proxy server in conjunction with the SmartFilter product.) The text of the page states that the requested Web site could not be found (an HTTP 404 error).[81] However, when we compared this with the HTTP headers returned in response to our request for www.tunezine.com, we found that the actual error was a 403 error, which indicates that the request is prohibited.[82] Thus, we conclude that Tunisia is deliberately misrepresenting to its users why they cannot reach filtered sites by claiming that these sites do not exist, rather than indicating that they are blocked.

---

[81] *See* R. Fielding et al., *Hypertext Transfer Protocol – HTTP 1.1: 10 Status Code Definitions*, *at* http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html (stating that the 404 error code is displayed when the "server has not found anything matching the Request-URI").

[82] *See id.* (defining the "403 Forbidden" error code for HTTP). The header ONI received was "HTTP/1.x 403 Forbidden," while the block page indicates a 404 error.