OpenNet Initiative Bulletin

West Censoring East

The Use of Western Technologies by
Middle East Censors
2010-2011

Executive Summary

The OpenNet Initiative has documented network filtering of the Internet by national governments in over forty countries worldwide. Countries use this network filtering as one of many methods to control the flow of online content that is objectionable to the filtering governments for social, political, and security reasons. Filtering is particularly appealing to governments as it allows them to control content not published within their national borders.

National governments use a variety of technical means to filter the Internet; in this paper, we analyze the use of American- and Canadian-made software for the purpose of government-level filtering in the Middle East and North Africa.

In this report, the authors find that nine countries in the region utilize Western-made tools for the purpose of blocking social and political content, effectively blocking a total of over 20 million Internet users from accessing such websites.[1] The authors analyze as well the increasing opacity of the usage of Western-made tools for filtering at the national level.

Helmi Noman and Jillian C. York authored this report. ONI principal investigators Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain authored the foreword.

Noman is a Senior Research Fellow at the Munk School of Global Affairs, University of Toronto, and is a Berkman Center Research Affiliate. York is the coordinator for the OpenNet Initiative at the Berkman Center for Internet & Society.

The authors would like to thank James Tay of Citizen Lab for technical support and test data analysis.

About the OpenNet Initiative

The OpenNet Initiative is a collaborative partnership of three institutions: the Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa).

ONI's mission is to investigate, expose and analyze Internet filtering and surveillance practices in a credible and non-partisan fashion. We intend to uncover the potential pitfalls and unintended consequences of these practices, and thus help to inform better public policy and advocacy work in this area. For more information about ONI, please visit http://opennet.net.

Foreword

Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain

Internet filtering can take place as parents and schools shield children from harmful content, businesses enforce workplace standards for employees, and governments seek to shape and control the flow of information to and from their citizens. Over a decade ago Lawrence Lessig warned of the "vertical portability" of tools to manage and enforce such filtering: "This alternative is often praised as a 'private' or 'user-empowering' solution to the indecency problem. URL-blocking software such as SurfWatch or Cybersitter, which works by restricting access to specific addresses, was the first version of this idea. More recently, in response to cyberporn hysteria, the World Wide Web Consortium has developed a sophisticated technology called the Platform for Internet Content Selection, or PICS. Blocking software is bad enough—but in my view, PICS is the devil."[2] If care were not taken, technologies to protect children using a handful of PCs could be readily repurposed to engage in mass political and other censorship affecting millions of people.

Today that portability is amply shown but rarely discussed. Filtering technologies produced by companies, some Fortune 500, in the United States and Canada are currently being repurposed for state-sanctioned censorship. This is not simply a case of a general purpose, neutral tool being used for an end not contemplated by its maker. The filtering products of today engage in regular communications with their makers, updating lists of millions of websites to block across dozens of content categories, including political opposition and human rights. When McAfee Smartfilter or Websense do their utmost to maintain lists of non-profit and advocacy groups their efforts directly affect what citizens in some authoritarian regimes can and cannot access online.

At least one company—Websense—has gone on record opposing the use of its software for the purposes of government censorship, except for the protection of minors from pornography. Our research indicates Websense appears to remain in use for censorship at least as of August 2010 despite those statements. Websense's competitors have not articulated a policy about censorship at all.

Censorship of search engine results at the behest of national governments by companies like MSN and Google has proven controversial, even as there the firms could point out that the purpose of a search engine is to provide access to information. They have, at various times, made the case that access to 99% of a corpus is more meaningful for freedom of expression than a failure to provide access to the remaining 1%. There is no counterpart argument for tools whose sole purpose is to filter—to privatize the censorship function, creating an assembly line of content that could be found objectionable by anyone, globally blockable by a government that need only check boxes to determine what to withhold from its citizens.

This report details just how popular Western filtering tools and services are among authoritarian regimes. As Internet controls grow worldwide, so too has the market for filtering tools and services. Their use is pervasive—even as it is becoming more opaque. Users who were formerly informed of the vendor prohibiting their access to a desired website are no longer told who is selecting what they can see and do online.

We hope that this report can inform a genuine discussion of the ethics and practice of providing national censorship technology and services, one that might lead to guidelines consonant with the most basic principles of freedom of expression.

Key Findings

At least nine Middle Eastern and North African state censors use Western-built technologies to impede access to online content. ISPs in Bahrain, UAE, Qatar, Oman, Saudi Arabia, Kuwait, Yemen, Sudan, and Tunisia use the Western-built automated filtering solutions to block mass content, such as websites that provide skeptical views of Islam, secular and atheist discourse, sex, GLBT, dating services, and proxy and anonymity tools. These lists of sites are maintained by the Western company vendors. The ISPs also use these tools to add their own selected URLs to the companies' black lists.

At least three national ISPs—Qatar's Qtel, UAE's du, and Yemen's YemenNet—currently employ the Canadian-made commercial filter Netsweeper. Netsweeper Inc. does not seem to take issue with governments implementing political and religious censorship using their tools, and acknowledges working with telecom operators in Qatar, UAE, Yemen, India, and Canada. The company says its product can be used to block inappropriate content to meet government rules and regulations "based on social, religious or political ideals."[3]

Contrary to Netsweeper, Websense offers a stated policy that it does not provide governments with mass filtering tools except in cases where government policy required filtering of pornography. However, ONI found that Yemen's government-run ISP YemenNet has used Websense to implement filtering of political and social content.

Saudi Arabia, UAE, Kuwait, Bahrain, Oman and Tunisia have used American-made SmartFilter products now owned by Intel. Intel's SmartFilter management does not have a publically declared policy on the use of its products by governments to implement censorship.

ISPs using commercial filters are increasingly obscuring that face as their citizens surf the Web and encounter blocks. A few years ago, the blockpages from many countries' ISPs and their corresponding html source files had references to the commercial filters. Recent ONI research found that now more ISPs attempt to leave in their blockpages no attribution of the products in use.

ONI and others have documented ongoing mis-categorization of websites and overreach of lists.[4]

Introduction

Filtering technology built by Western companies has been used by at least nine Middle Eastern and North African state censors to impede access to and engagement in free speech. These companies not only provide the technology infrastructure but also provide ongoing access to lists that categorize millions of URLs for the purposes of filtering. Often pitched in the first instance for use by parents, schools, and workplaces, these technologies can also be sold to make filtering easy for entire countries: Once the underlying infrastructure is set up, the censors need only activate the tool and select the categories they wish to censor. The companies that produce these tools often bundle them with solutions that are meant to protect computer networks from malicious software such as viruses and malware; this is a potentially dangerous proximity between two different concepts that can have a serious impact on free speech.

Regulations and accountability related to the use of commercial filters and services for state censorship are typically non-existent, and there is no or little oversight from civil society and free speech advocacy groups on the role Western technology companies play in restricting access to content online.

Regimes rely on such software to censor content they deem objectionable, though what a regime sees as objectionable can—and often does—fall within the range of speech protected by international frameworks such as Article 19 of the Universal Declaration of Human Rights.[5] Websites promoting nonviolent dissension, as well as social networking sites, are among those often censored by the regimes using such software.

Furthermore, the filtering companies typically rely on error-prone methods to categorize websites. Though some companies enable the public to check how a given URL is categorized within their respective databases, and some allow users to suggest alternative categorizations, this seemingly participatory approach is fragile if not run by professionals versed in world languages who can prevent orchestrated efforts to abuse the system.

By relying upon out-of-the-box filtering systems, states have outsourced the task of deciding what is or is not acceptable speech. In addition, filtering software enables state censors to overlay their own censorship decisions on top of that of the vendors. This paper highlights how filtering solutions produced in the West have a tangible impact on the flow of information in non-Western countries, especially those in the Middle East and North Africa region.

Mass filtering

Since 2002, ONI has found evidence of the use of automated filtering solutions used to block mass content across various categories.[6] In the Middle East and North Africa, several state-run ISPs have been found to use such software to block topics related to sexual content, nudity, LGBT content, dating sites, and privacy tools and anonymizers.

The mass blocking of such sites has been supported in many countries through the use of Western commercial products, which provide both the software and continuously updated content known as category-based filtering. For example, McAfee SmartFilter[7] maintains an online database with over 25 million websites that can be blocked in over 90 categories.

ISPs can also easily create user-defined categories that allow them to block websites not included in the provided database.

McAfee SmartFilter's categories are comprehensive. They are:[8]

- Alcohol
- Anonymizers
- Anonymizing
- Art / culture /
- Auction / classifieds
- Blogs / wikis
- Business
- Chat
- Content server
- Criminal activities
- Dating / social
- Digital postcards
- Drugs
- Education / reference
- Entertainment
- Extreme
- Fashion / beauty
- Finance / banking
- For kids
- Forum / bulletin boards
- Gambling
- Gambling related
- Game / cartoon violence
- Games
- General news
- Government / military
- Gruesome content
- Hacking / computer crime
- Hate / discrimination
- Health
- Historical revisionism
- History
- Humor / comics
- Illegal software
- Incidental nudity
- Information security
- Instant messaging
- Interactive web applications
- Internet radio / TV
- Internet services
- Job search
- Malicious sites
- Marketing / merchandising
- Media downloads
- Media sharing
- Messaging
- Mobile phone
- Moderated
- Non-profit / advocacy groups
- Nudity
- Online shopping
- P2P / filesharing
- Parked domain
- Personal network storage
- Personal pages
- Pharmacy
- Phishing
- Politics / opinion
- Pornography
- Portal sites
- Profanity
- Provocative attire
- Public information
- Real estate
- Recreation / hobbies
- Religion and ideology
- Remote access
- Resource sharing
- Restaurants
- School cheating information
- Search engines
- Sexual materials
- Shareware / freeware
- Software / hardware
- Spam email URLs
- Sports
- Spyware / adware
- Stock trading
- Streaming media
- Technical information
- Technical / business forums
- Text / spoken only
- Tobacco
- Travel
- Usenet news
- Violence
- Visual search engine
- Weapons
- Web ads
- Web mail
- Web phone

In addition to category-based filtering, McAfee SmartFilter also provides reputation-based filtering based on data collected by McAfee that determine reputation scores and category placement on potentially malicious behavior of websites that could expose a computer network to viruses, malware, and other security risks.

Websense also has a comprehensive database of over 26 million websites, in over 90 URL categories, representing more than 50 languages. Websense's URL classification relies on human inspection in addition to proprietary classification software.

Websense's URL categories are:[9]

Abortion
- Pro-Choice
- Pro-Life

Adult Material
- Adult Content
- Lingerie and Swimsuit
- Nudity
- Sex
- Sex Education

Advocacy Groups
Business and Economy
Financial Data and Services
Hosted Business Applications
Drugs
- Abused Drugs
- Marijuana
- Prescribed Medications
- Supplements and Unregulated Compounds

Education
- Cultural Institutions
- Educational Institutions
- Educational Materials
- Reference Materials

Entertainment
- MP3 and Audio Download Services

Gambling
Games
Government
- Military
- Political Organizations

Health
Illegal or Questionable
Information Technology
- Computer Security
- Hacking
- Proxy Avoidance
- Search Engines and Portals
- URL Translation Sites
- Web & Email Spam
- Web Collaboration
- Web Hosting

Internet Communication
- Web Chat
- General Email
- Organizational Email
- Text and Media Messaging

Job Search
Militancy and Extremist
Miscellaneous
- Content Delivery Networks
- Dynamic Content
- File Download Servers
- Image Servers
- Images (Media)
- Network Errors
- Private IP Addresses
- Uncategorized

News and Media
- Alternative Journals

Parked Domain
Racism and Hate
Religion
- Non-Traditional Religions and Occult and Folklore
- Traditional Religions

Shopping
- Internet Auctions
- Real Estate

Social Organizations
- Professional and Worker Organizations
- Service and Philanthropic Organizations
- Social and Affiliation Organizations
- Society and Lifestyles
- Alcohol and Tobacco
- Blogs and Personal Sites
- Gay or Lesbian or Bisexual Interest
- Hobbies
- Personals and Dating
- Restaurants and Dining
- Social Networking
- Social Networking and Personal Sites
- Special Events

Sports
- Sport Hunting and Gun Clubs

Tasteless
Travel
User-Defined
Vehicles
Violence
Weapons

ISPs and the governments to whom they answer use the same software to add websites manually to vendor-updated block lists. These manually-added sites include country-specific or general oppositional content, especially those in local languages. We have found that state ISPs do in fact block local political oppositional content that has not been picked up by the commercial filters' databases. This content includes local and country-specific forums, blogs, and websites. Moreover,

we have found that the commercial filters do not pick up Arabic content as comprehensively as content in English.[10]

Our previously published research[11] found that, to one degree or another, Saudi Arabia, UAE, Kuwait, Bahrain, and Oman use SmartFilter technology to block content across content categories such as websites that provide critical views of Islam, secular and atheist discourse, sex, GLBT, dating services, and proxy and anonymity tools. Tunisia also blocked content in these categories until January 2011, when an uprising led to diminishment of the country's filtering regime. ONI tests conducted after January 2011 showed that the authorities there no longer block political websites; however they continue to conduct filtering of social sites. In fact, a January 22, 2011 statement from the Secretariat of State for Information Technologies said that access to all websites had been restored except for "sites with indecent content, comprising violent elements or inciting hatred."[12]

Also, to varying degrees, these states have also been found to block political content and oppositional websites.

Using Websense, Yemen's main ISP was found to block the same content categories, and at some point also blocked the use of the keywords "sex" and "porn", along with other suggestive terms in search strings. Using McAfee's SmartFilter, the UAE continues to prevent the use of keywords that can potentially render explicit content.

Testing in January 2011 indicated that Yemen's ISP YemenNet, Qatar's Qtel, and the UAE's du, have been using the commercial Web filter Netsweeper. Earlier research showed that Qtel has used SmartFilter and YemenNet has used Websense. We are, however, unable to technically verify if du has used a different solution in the past. UAE's other ISP, Etisalat, has been found to use SmartFilter.[13]

Netsweeper does not seem to take issue with governments implementing political and religious censorship using their tools. The company says that its product can be used to "block inappropriate content using [sic] preestablished list of 90+ categories to meet government rules and regulations—based on social, religious or political ideals."[14] The company acknowledges that its product is being used by telecom providers in countries known for pervasive censorship practices such as Qatar, Yemen, and the United Arab Emirates.[15]

At least two major telecom providers in India also use Netsweeper for Internet filtering. Tata Communications, formerly known as Videsh Sanchar Nigam,[16] announced in 2007 the launch of Tata Indicom's Web Protect, which in collaboration with Netsweeper "enables users to block access to specific websites, chat rooms or any other unwanted content."[17] ONI test however has found no evidence that Netsweeper is being used to enforce mandatory censorship.

The other Indian telecom provider, BSNL (Bharat Sanchar Nigam Ltd.), "uses the Netsweeper Enterprise Filter as the interceptor, with all the network traffic … going through the filter," according to a BSNL Case Study produced by Netsweeper.[18] The case study says that "[g]overnments are cracking down on illegal content on web sites. BSNL, India's largest telco, selected Netsweeper as the technology to meet Federal content regulations."

Other Western-built filtering solutions have also been deployed by national ISPs in the region, but ONI cannot determine to what extend these systems are being used for filtering. For example,

Saudi Arabia's Internet gateway—Internet Services Unit (ISU) at King Abdulaziz city for Science & Technology (KACST)—has used America-made Blue Coat ProxySG appliances to protect against malicious content and provide a "productive Internet experience," according to a case study published by Blue Coat.[19] Blue Coat products support content filtering providers including SmartFilter,[20] the solution used by Saudi Arabia's Internet gateway. ONI previously published research found that Yemen's ISP YemenNet has used a Blue Coat integrated cache/filter appliance to run Websense.[21]

The mass use of commercial filters: Leave no traces

ISPs using commercial filters are increasingly obscuring that fact. A few years ago, blockpages and their corresponding html source code had references to the commercial filter being used. We have since found that more ISPs have cleansed such references from the Web surfing experience.

For example, UAE ISP du's blockpage source code had earlier in 2010 a hint as to the commercial filter. The blockpage source code included the URL http://94.201.251.238/webadmin/start/, which is the link to the Netsweeper management interface. Similarly, Qatar's Qtel, had the same reference page on its own blockpage, http://82.148.98.52:8080/webadmin/deny/index.html.

Though Yemen's YemenNet no longer shows in its blockpage the name of the commercial filter, our examination of the blockpage source code found a clue that enabled us to generate the Netsweeper management page installed in the local servers (See figure 1).

Moreover, some ISPs' blockpages used to have the logo or the name of commercial filter they used. Saudi Arabia's Saudi Telecom's blockpage in 2009 printed the name and logo of SmartFilter for some objectionable websites. (See figure 2).

The Saudi authorities then announced a new standard blockpage after supervision of Internet filtering in the country was transferred from King Abdul Aziz City for Science and Technology (KACST) to the state Communications and Information Technology Commission (CITC). The blockpage announced by the authorities[22] had no reference as to what software the ISPs use (See figure 3).

Other countries such as Libya, Morocco, and Jordan also implement Internet censorship to various degrees, but we have not determined whether any of these countries use the software highlighted in this paper. In Syria, we found that ISPs such as Inet, Teranet, and Zad have used Squid as a proxy tool to block access to objectionable websites that included oppositional Web content. Squid is a free software package released under the GNU General Public License that was funded by the National Science Foundation.[23] It is a caching proxy that is built to reduce bandwidth and improve response times by caching and reusing frequently-requested Web pages, however, ISPs in Syria have repurposed it for Internet censorship.

It is important to note that due to the fact that some ISPs have switched commercial filters and now attempt to leave no indication of what commercial filters are being used, ONI can only verify that the commercial filtering solutions mentioned above have at one time been used by the respective ISPs.

Figure 1: Screen shot of Netsweeper Business login page installed in YemenNet server

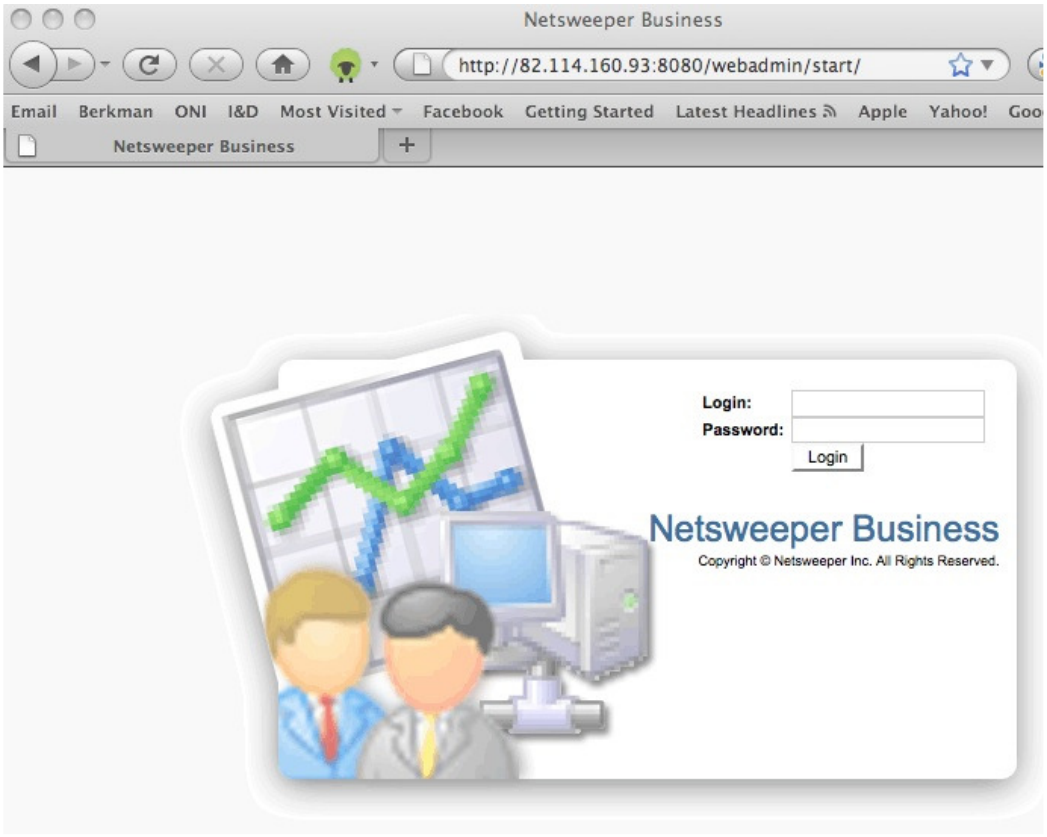


Figure 2: Saudi Arabia's STC blockpage in 2009

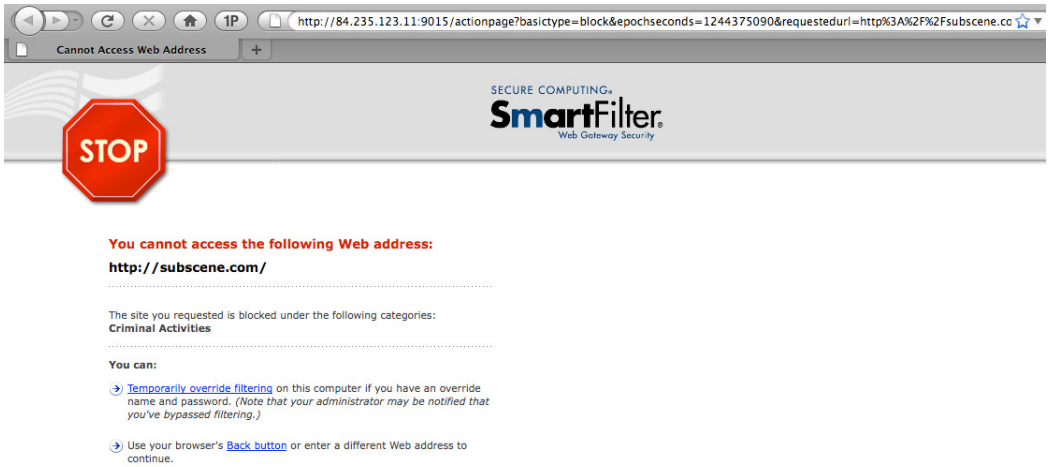
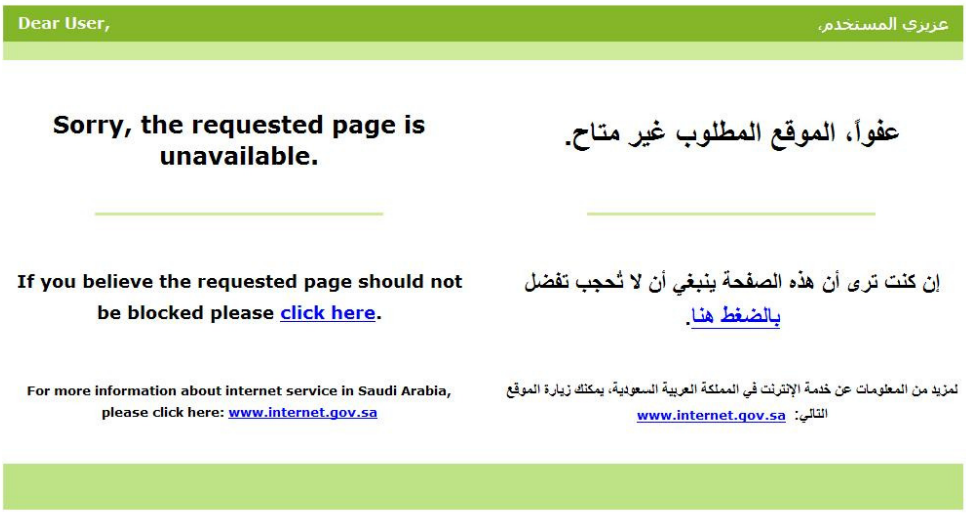


Figure 3: Saudi Arabia's ISPs standard



blockpage

Figure 4: Qatar's Qtel blockpage

Figure 5: UAE's du blockpage

URL Mis-Categorization and Websense

Websense, US-based filtering software used by Yemen's primary ISP YemenNet to filter the Internet, sells not only the software but also ongoing access to a database of millions of URLs in over 90 categories. As is inevitable with any mass filtering software applied to a huge and rapidly changing universe of websites, the company has made erroneous and inaccurate URL categorizations. As a result, and on top of government-level intentional filtering, users in countries where censorship is prevalent are often prevented from accessing content that was not intentionally filtered.

In 2009, the ONI reported that Yemen was using filtering software from US –based company Websense to filter websites across several categories, including pornography, sex education materials, and anonymizing and privacy tools.[24]

However, Websense's stated policy is to not provide governments with censorship tools and services except in the limited case where government policy requires filtering of pornography.[25] Its policy states:

> **Websense does not sell to governments or Internet Service Providers (ISPs) that are engaged in any sort of government-imposed censorship.** Any government-mandated censorship projects will not be engaged by Websense. If Websense does win a business and later discovers that the government is requiring all of its

> national ISPs to engage in censorship of the Web and Web content, we will remove our technology and capabilities from the project. Websense does however, provide filtering services in response to "global filtering" projects where the government mandated policy (1) prohibits minors from accessing pornography and/or (2) prohibits child pornography. With the above guidelines in place an example scenario would be if a government wants to prevent minors from seeing pornography at the ISP level. If that government then requires all ISPs to block adult content from all users, but permits an adult user to gain access to that content after providing proof of age, then this is a project that Websense can participate in. Websense, however, does not engage in any arrangements with foreign governments (or government-imposed arrangements) that could be viewed as oppressive of rights.

When we contacted Websense about the use of its tools in Yemen for broader filtering, we were told:[26]

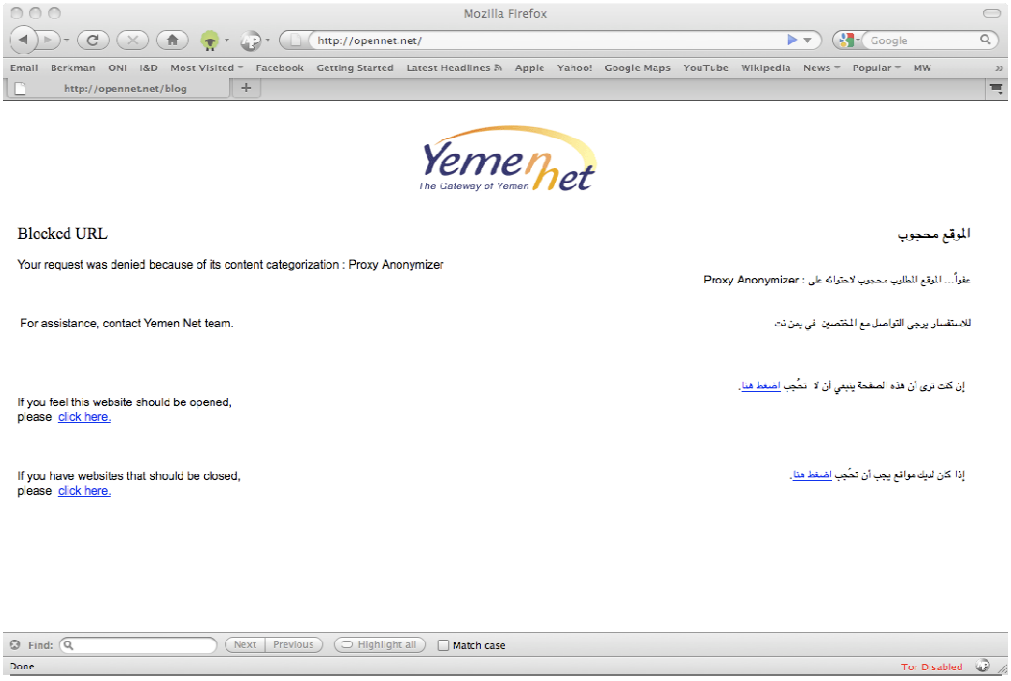
> Since we were informed about the potential use of our products by Yemeni ISPs based on government-imposed Internet restrictions in Yemen, we have investigated this potential non-compliance with our anti-censorship policy. Because our product operates based on a database system, we are able to block updated database downloads to locations and to end users where the use of our product would violate law or our corporate policies. We believe that we have identified the specific product subscriptions that are being used for Web filtering by ISPs in Yemen, and in accordance with our policy against government-imposed censorship http://www.websense.com/content/censorship-policy.aspx, we have taken action to discontinue the database downloads to the Yemeni ISPs.

Despite Websense's response, in August 2010 the ONI found that its website at http://opennet.net was blocked by Yemen's primary ISP, the state-run YemenNet. The blockpage served by the ISP read: "Your request was denied because of its content categorization: Proxy Anonymizer."

To be sure, ONI is not a proxy tool service and does not offer the use of circumvention tools. Rather, it is an academic research organization that investigates, exposes and analyzes Internet filtering and surveillance practices in a credible and non-partisan fashion.

ONI investigated the blocking incident and found out that Websense had indeed categorized ONI as a "Proxy Avoidance" website. See Appendix I for ONI's interrogation of Websense database.

Figure 6: Yemen ISP YemenNet's blockpage showing categorization of ONI website as "proxy anonymizer"

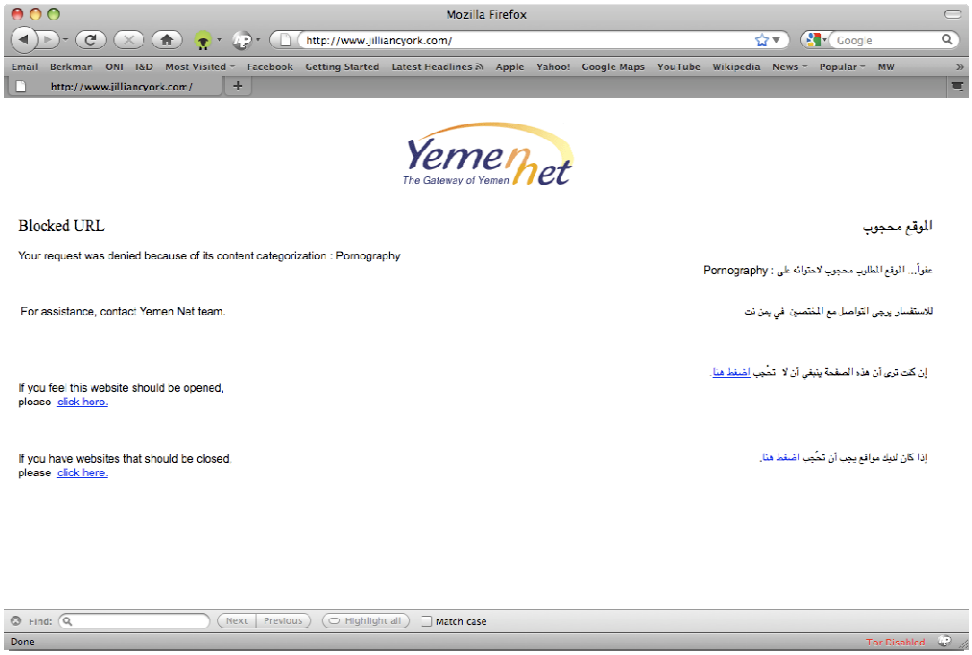


Approximately 10 days after confirming that http://opennet.net was blocked in Yemen, the URL was re-categorized by Websense as an "Educational Institution." Shortly thereafter, the ONI site became accessible from Yemen. From this we may infer, but not definitively establish, that Websense categorizations were still being received and updated in Yemen as of August 2010.

We also learned that the personal website of this report's co-author Jillian York was blocked in Yemen shortly after a post entitled "Filtering Sex in the Arab World"[27] that referred to an earlier ONI paper entitled "Sex, Social Mores, and Keyword Filtering: Microsoft Bing in 'Arabian Countries,'" which analyzed keyword filtering by Microsoft's Bing search engine.[28] The post contained the terms "sex" and "LGBT". The ISP's blockpage reads, "Your request was denied because of its content categorization: Pornography".

Figure 7: Yemen ISP YemenNet blockpage showing categorization of Jillian C. York's personal website as

"pornography"



We checked how Websense categorizes the URL of Jillian's website using the IT Toolbox (https://toolbox.richland2.org/r2apps/r2websense), which provides an interface to Websense URL Lookup. We found out that York's website has been categorized as a "Sex" website.

The site without the www prefix (http://jilliancyork.com) is not categorized by Websense. We checked the URL without the "www" using Yemen's ISP YemenNet and found out that the URL is not blocked. This contributes to the inference that Websense tools and services remain in use in Yemen.

McAfee's SmartFilter

In 2006, ONI found that another filtering tool, SmartFilter, was being used by the governments of Saudi Arabia, the United Arab Emirates, and Iran to block various types of content.[29] SmartFilter was developed by Secure Computing, a US-based company that has since been acquired by McAfee.[30]

In 2005, ONI found that the government of Iran was using SmartFilter to filter a variety of websites across different categories, a discovery that the government of Iran confirmed.[31] Secure Computing, owner of SmartFilter responded:

> Secure Computing has sold no licenses to any entity in Iran, and any use of Secure's software by an ISP in Iran has been without Secure Computing's consent and is in violation of Secure Computing's End User License Agreement. We have been made aware of ISPs in Iran making illegal and unauthorized attempts to use of our software. Secure Computing is actively taking steps to stop this illegal use of our products. Secure Computing Corporation is fully committed to complying with the export laws, policies and regulations of the United States. It is Secure Computing's

> policy that strict compliance with all laws and regulations concerning the export and re-export of our products and/or technical information is required. Unless authorized by the US Government, Secure Computing Corporation prohibits export and reexport of Secure products, software, services, and technology to Iran and destinations subject to US embargoes or trade sanctions.[32]

In 2005, Secure Computing responded to the ONI's observations that its products were being used in Iran by stating that it had not sold SmartFilter to the Iranian government—something that would be prohibited by US export control policy[33] -- but that the company does sell to foreign ISPs as the law allows.[34]

ONI also determined that Sudan, Oman, and Tunisia were using SmartFilter.[35]

Unlike Websense, SmartFilter does not publish a policy on its use at the government level. McAfee's Code of Business Conduct and Ethics does not mention government use of filtering products.[36]

URL Mis-Categorization in McAfee SmartFilter

Like Websense, McAfee's SmartFilter relies on artificial intelligence techniques that include content analysis as part of the URL categorization process.

According to McAfee, "The categorization of a particular URL is a defined process using objective standards and definitions. To gather and rate potential websites, McAfee uses various technologies, artificial intelligence techniques, such as link crawlers, security forensics, honey pot networks, sophisticated auto-rating tools, and customer logs."[37]

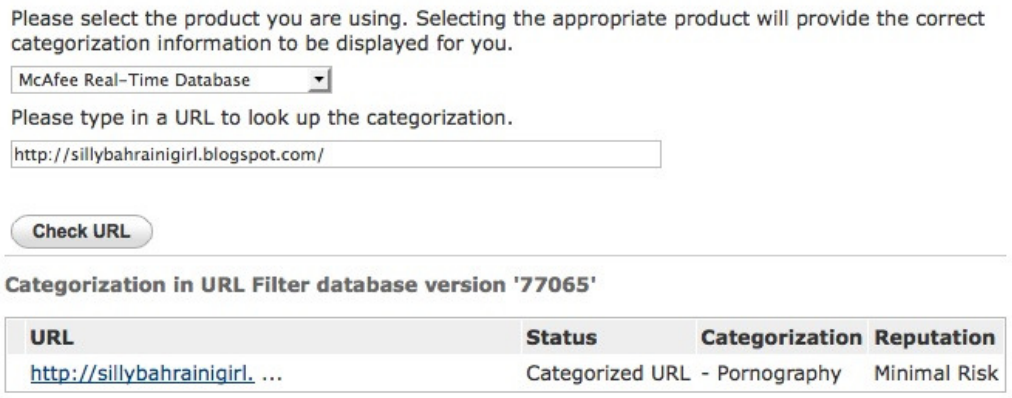
ONI has documented mis-categorization of high-profile URLs such as the microblogging service http://www.twitter.com, the Internet Radio website http://www.last.fm/, and the blogging platform http://www.livejournal.com. All of these websites were categorized by SmartFilter database as "dating" websites. As a result, they were made inaccessible in some countries in the Middle East and North Africa (e.g., the United Arab Emirates) which block dating websites.

Figure 8: A screenshot of SmartFilter's URL database shows how URLs were categorized in June 2008

URL	Status	Categorization	Reputation
http://www.last.fm/	Categorized URL	- Entertainment - Dating/Social Networking - Streaming Media	Neutral
http://www.livejournal.co ...	Categorized URL	- Dating/Social Networking - Blogs/Wiki	Neutral
http://www.orkut.com/	Categorized URL	- Instant Messaging - Dating/Social Networking - Web Mail - Media Sharing	Neutral
http://www.twitter.com/	Categorized URL	- Dating/Social Networking	Neutral

In January 2011, Amira al-Hussaini, Global Voices Online Middle East and North Africa Editor reported that her blog, "Silly Bahraini Girl," had been blocked in Bahrain.[38] ONI investigation found that the site has indeed been blocked not only in Bahrain but also in the UAE and Kuwait. All three countries use SmartFilter to block websites across a variety of categories. Further examination revealed that in fact the site has been mis-categorized by the filtering software as "pornography," a category that is blocked by the three countries, as well as other regimes in the region.

Figure 9: A screenshot of the record for al-Hussaini's website in SmartFilter's URL database



Conclusion

Despite documentation by the ONI and other research and advocacy organizations, little discussion has taken place in the public sphere on the use of Western technologies for government-level filtering.

While Websense has publicly stated that its software is not meant for use by governments, such use may be taking place, and other companies appear to have done little to curb the use of their tools—if not offering them outright for that purpose—for government-level censorship. These companies seem not to have adopted policies and procedures to safeguard freedom of expression in the event that states rather than parents and schools use their tools, as their products are being openly used by several state-run ISPs to limit what citizens can and cannot access online. That Netsweeper publically declares that it offers its software for use to implement government censorship on political and religious grounds highlights the fact that there is currently no effective accountability system on the practices of the commercial software companies vis-à-vis human rights. Western government leaders have advocated for human rights and the free flow of information in heavily censored countries, but we have yet to see concrete initiatives from these governments to address how Western companies are directly collaborating with—and perhaps profiting from—the government censors.

Western companies are playing a role in the national politics of many countries around the world. By making their software available to the regimes, they are potentially taking sides against citizens and activists who are prevented from accessing and disseminating content thanks in part to filtering software.

Moreover, the commercial filters place content filtering too close to conceptually different computer network security solutions. Bundling category-based content censorship with anti-virus

and anti-malware network protection tools poses a risk to the future of free speech. This close proximity of two different solutions in one package invites content services provides and Internet service providers who seek to protect their computer networks from malicious software to also consider content-based censorship.

Though the above represents three disparate problems, the optimal solution lies with the leadership of companies that produce filtering software. Such companies must recognize the role their tools play in the international landscape and set forth policies that protect Internet users' right to free expression—or at least put them on record about the role that they play.

Notes

[1] 20 million is the number of Internet users in Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, Sudan, Tunisia, the United Arab Emirates, and Yemen, as estimated by the World Bank.
[2] Lawrence Lessig, Tyranny in the Infrastructure, Wired, July 1997 http://www.wired.com/wired/archive/5.07/cyber_rights.html.
[3] Netsweeper, Netsweeper Overview For Telcos http://www.netsweeper.com/site/index.php?page=downloads&type=entry&id=51&root=1&keep_session=1986028676.
[4] See for example "Censorware makers behind SmartFilter block Daily Kos," BoingBoing, October 4, 2006, http://www.boingboing.net/2006/10/04/censorware_makers_be.html.
[5] The Universal Declaration of Human Rights, http://www.un.org/en/documents/udhr/index.shtml.
[6] See ONI country studies at http://www.opennet.net.
[7] As of August 2010, McAfee is now owned by Intel; Ashlee Vance, "With McAfee Deal, Intel Looks for Edge," *New York Times*, August 19, 2010, http://www.nytimes.com/2010/08/20/technology/20chip.html.
[8] McAfee SmartFilter Data Sheet, http://www.mcafee.com/us/resources/data-sheets/ds-smartfilter.pdf.
[9] Websense, URL Categories, http://www.websense.com/content/urlcategories.aspx.
[10] Helmi Noman, "Regional Overview of Filtering Practices in the Middle East and North Africa," OpenNet Initiative, August 7, 2009, http://opennet.net/research/regions/mena.
[11] See ONI country studies at http://www.opennet.net.
[12] Tunisian News Agency, "Free access to all websites except indecent ones," January 22, 2011, http://www.tap.info.tn/en/index2.php?option=com_content&do_pdf=1&id=14258.
[13] See 2009 ONI countries studies at http://www.opennet.net.
[14] Netsweeper, Netsweeper Overview For Telcos, http://www.netsweeper.com/site/index.php?page=downloads&type=entry&id=51&root=1&keep_session=1986028676.
[15] Ibid.
[16] Tata, VSNL renamed as Tata Communications, December 15, 2007, http://www.tata.com/article.aspx?artid=JSsSkB13v9Q.
[17] Tata, VSNL launches Tata Indicom Web Protect, July 20, 2007, http://www.tata.com/article.aspx?artid=0y3l14QUBqQ.
[18] Netweeper Inc., BSNL Case Study, http://www.netsweeper.com/site/index.php?page=downloads&type=entry&id=5&root=1.
[19] Blue Coat Systems, Case Study – KACST, http://www.bluecoat.com/document/case-study-kacst.
[20] Blue Coat Systems, Blue Coat Introduces ProxySG™ — Secure Proxy Appliances Control User Communications Over the Web, September 8, 2003, http://www.bluecoat.com/news/pr/109.
[21] OpenNet Initiative, "Country Profile: Yemen," August 7, 2009, accessed November 17, 2010, http://opennet.net/research/profiles/yemen.
[22] Communications and Information Technology Commission, New block page, http://www.internet.gov.sa/news/new-block-page/view?set_language=en.
[23] See info about Squid, http://www.squid-cache.org/Intro/.
[24] OpenNet Initiative, "Country Profile: Yemen," August 7, 2009, accessed November 17, 2010, http://opennet.net/research/profiles/yemen.
[25] Websense Policy on Government-Imposed Censorship, accessed August 12, 2009, http://www.websense.com/content/censorship-policy.aspx.

[26] Jillian C. York, "Websense Bars Yemen's Government from Further Software Updates," OpenNet Initiative Blog, August 12, 2009, accessed November 17, 2010, http://opennet.net/blog/2009/08/websense-bars-yemens-government-further-software-updates.
[27] Jillian C. York, "Filtering Sex in the Arab World," May 3, 2010, http://jilliancyork.com/2010/03/05/filtering-sex-in-the-arab-world/.
[28] Helmi Noman, OpenNet Initiative, "Sex, Social Mores, and Keyword Filtering: Microsoft Bing in the 'Arabian Countries,'" March 4, 2010, http://opennet.net/sex-social-mores-and-keyword-filtering-microsoft-bing-arabian-countries.
[29] Nart Villeneuve, "The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace," First Monday 11:1-2 (2006), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227.
[30] Secure Computing, "McAfee, Inc. Agrees to Acquire Secure Computing," September 22, 2008, accessed November 17, 2010, http://www.securecomputing.com/news_display.cfm?nid=1549.
[31] OpenNet Initiative, "Internet Filtering in Iran 2004-2005: A Country Study," 2005, http://opennet.net/studies/iran.
[32] Ibid.
[33] Bureau of Industry and Security, U.S. Department of Commerce, "Introduction to Commerce Department Export Controls," accessed November 17, 2010, http://www.bis.doc.gov/licensing/exportingbasics.htm; United States Department of Treasury, "Iran Sanctions," accessed November 17, 2010, http://www.ustreas.gov/offices/enforcement/ofac/programs/iran/iran.shtml.
[34] BoingBoing, "ISPs in Iran, Tunisia also use SmartFilter (which blocks BoingBoing as 'nudity')," February 27, 2006, accessed November 17, 2010, http://boingboing.net/2006/02/27/isps_in_iran_tunisia.html.
[35] Ron Deibert et al., *Access Denied: The Practice and Policy of Global Internet Filtering*, (Cambridge: MIT Press, 2008), 15.
[36] McAfee Inc., "Code of Business Conduct and Ethics," March 4, 2004, http://www.mcafee.com/us/local_content/media/mcafee_standards_of_conduct.pdf.
[37] McAfee® TrustedSource™ Web Database, Reference Guide.
[38] Amira Al Hussaini, "My Blog is Blocked in Bahrain," *Silly Bahraini Girl*, January 4, 2011, http://sillybahrainigirl.blogspot.com/2011/01/my-blog-is-blocked-in-bahrain.html

Appendix I

The following is the result of our Websense database interrogation using a trial version of Websense. (See lines #7, 8, and 9):

```
C:\Program Files\Websense\bin>websenseping -m 8 -url opennet.net

----------------------------------------
Sending HTTP_LOOKUP_REQUEST...
----------------------------------------
URL = http://opennet.net
User Name =
Source IP = 0.0.0.0
Destination IP = 128.103.64.74
Disposition = CATEGORY_BLOCKED
Lookup Code = WISP_URL_BLOCKED
Category = Proxy Avoidance
Lookup Type = 0
Protocol ID = 1
Run Analytics = False
Logging Code = 1
Protocol Cache TTL = 0
URL Cache Cmd = 0
URL Cache Type = 0
URL Cache TTL = 0

Block Message =

Elapsed Time = 1 ms

AVG TIME PER REQUEST = 1 ms

C:\Program Files\Websense\bin>
```