
The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace**by Nart Villeneuve**

Abstract

Increasingly, states are adopting practices aimed at regulating and controlling the Internet as it passes through their borders. Seeking to assert information sovereignty over their cyber-territory, governments are implementing Internet content filtering technology at the national level. The implementation of national filtering is most often conducted in secrecy and lacks openness, transparency, and accountability. Policy-makers are seemingly unaware of significant unintended consequences, such as the blocking of content that was never intended to be blocked. Once a national filtering system is in place, governments may be tempted to use it as a tool of political censorship or as a technological “quick fix” to problems that stem from larger social and political issues. As non-transparent filtering practices meld into forms of censorship the effect on democratic practices and the open character of the Internet are discernible. States are increasingly using Internet filtering to control the environment of political speech in fundamental opposition to civil liberties, freedom of speech, and free expression. The consequences of political filtering directly impact democratic practices and can be considered a violation of human rights.

Contents[Introduction](#)[Borders in cyberspace](#)[Transparency, openness and accountability](#)[Unintended consequences](#)[Mission creep](#)[Conclusion](#)

Introduction

The Internet once presented a promise of abundant, unfiltered information that posed a challenge to the monopoly of conventional methods of communication and forms of information dissemination and control. These challenges, to both state and corporate actors, include use of the Internet as a publishing platform, a personal communications medium and as an economic vehicle. Bloggers, citizen journalists and independent media are viable competitors to traditional corporate and state-owned media. In the economic realm, Voice-Over-Internet-Protocol (VoIP) [1] is threatening to traditional telecommunications companies while offshore gambling and banking sites challenge existing laws and regulations. File-sharing services have significantly impacted the area of copyright and intellectual property. And, from the security perspective, spam, child pornography, identity theft, computer break-ins and terrorism — both cyberterrorism and the use of the Internet for recruitment — present significant challenges for governments worldwide.

Although decentralized, there are locations at the intersection of regulatory and technological controls through which an information control policy is imposed on the Internet. This is accomplished through a combination of technical and regulatory means including laws, licensing regimes, industry self-regulation, national filtering, and content removal which combine to create a matrix of control. Filtering is the technical mechanism through which such controls are operationalized.

States are adopting practices aimed at regulating and controlling the Internet as it passes through their borders. Much like geographical boundaries, states are seeking to assert information sovereignty over the Internet. While the Internet does not necessarily conform to state boundaries, mechanisms of geographic content control are increasingly being implemented. Unlike more benign forms of filtering, ones in which individual users retain some level of choice and control, Internet content filtering at the national level is imposed on entire populations, often with little accountability. It is, in effect, an information control policy in which Web content, deemed to be undesirable, is censored through technical means.


The motivations for state-directed Internet filtering include those with:

- a specific emphasis on e-commerce: tax, copyright, VoIP
- a specific emphasis on children: child pornography, violence
- a specific emphasis on content
 - cultural: pornography and gambling
 - political: dissidents and independent media
 - security: (cyber)terrorism and hacking, circumvention

Filtering is often seen as a technical “quick fix” to the challenges posed by the rapid expansion of the Internet. Despite its numerous positive achievements, the Internet has created new security threats. In addition to computer and network security issues, information security has now become a paramount concern. In the same way that firewalls are deployed to protect systems from outside threats, Internet filtering technology attempts to prevent access to specific content. Filtering is used as a means to control external content, such as Web sites, that operate outside a country’s geographical territory [2].

However, there are significant unintended consequences that occur when filtering systems are deployed. Filtering has two inherent flaws: over-blocking and under-blocking. Filtering technologies are not only unable to block all targeted content, but they inevitably block content that was never intended to be blocked. At best, Internet filtering prevents casual or inadvertent access to designated content. In order to block content, specific sites must be identified and intentionally blocked [3]. Given the rapid growth of Internet content and the creation of new Web sites there will always be content that is not located and blocked even though it falls with a filtering technology’s blocking requirements. Filtering technology cannot keep pace with categorizing and blocking existing content, let alone all the newly created content on the Internet. Thus there will always be content available that is similar to blocked content.

Filtering systems can be easily circumvented by those actively seeking filtered content. There are numerous techniques and services through which users can access blocked content. Open proxy servers and private circumvention systems allow users to easily bypass Internet filtering by browsing through computers located in non-filtered locations. Anonymous circumvention systems allow users to bypass filtering anonymously and securely. While efforts can be taken to block common, publicly known circumvention systems, private circumvention systems remain effective and undetectable allowing users to freely browse any Internet content regardless of filtering.



In effect, the manufacturers of filtering software are determining what Internet content citizens of entire countries have access to. Not only do these companies often make mistakes, but their selection process is not open to peer review and scrutiny.

.....

There are significant transparency and accountability issues raised by the deployment of filtering technology. The process through which content is selected and blocked is most often conducted in secrecy. There is little accountability in the selection process and no mechanism for review or redress for incorrect blocking. There are several key issues with regard to the selection of content to be blocked. Countries rarely specifically state the exact criteria to be met in order to have a site blocked. Instead, the selection process is often vague and arbitrary and rarely is justification provided as to why a specific site is blocked. This problem is exacerbated when countries add their own block lists to existing commercial filtering technology. The block lists used by commercial filtering technology are kept private as they are the intellectual property of the manufacturer. Even the countries that deploy these products at the national level do not know what specific sites are blocked. In effect, the manufacturers of filtering software are determining what Internet content citizens of entire countries have access to. Not only do these companies often make mistakes, but their selection process is not open to peer review and scrutiny.

Filtering effectiveness is not rooted entirely in technology; the technical implementation of filtering forms the basis of new social norms in which users conform to accepted patterns of behavior and do not seek to access content known to be filtered. Thus filtering is often combined with policies intended to create fear and intimidation coercing users into self-censorship. As non-transparent filtering practices meld into forms of censorship the effect on democratic practices and the open character of the Internet are discernible. Citizens subjected to Internet filtering and surveillance grow to fear potential penalties for publishing or accessing content that may (or may not) be considered sensitive thereby limiting free communication and dialog.

Borders in cyberspace

Internet filtering technology allows controls to be placed on access to Internet content. Although the initial focus of such technology was on the individual level — allowing parents to restrict children’s access to inappropriate content — filtering technology is now being widely deployed at the institutional and national level. Control over access to Internet content is becoming a priority for a number of institutional actors including schools, libraries and corporations [4].

Content filtering technologies rely on list-based blocking, often in conjunction with blocking techniques that use keyword matching, to dynamically block Internet content. Lists of domain names and URLs are compiled and categorized then loaded into filtering software which can be configured to block only certain categories. When users attempt to access a Web page the filtering software checks its list database and blocks access if the page is on that list. If keyword blocking is enabled, the software will check each Web page (the domain, URL path and/or body content of the requested page) and dynamically block access to the page if any of the banned keywords are present.

When deployed at the national level, many states implement robust enterprise level filtering technology at Internet Service Providers (ISP) or near international gateway connections so that the filtering affects the entire country. These technologies can be deployed at any level of Internet access within a country with varying degrees of centralized coordination and control. It is quite common for states to require ISPs to implement filtering resulting in a situation in which filtering is not uniform across all points of network access. In other cases, the filtering regime is centralized and all users regardless of ISP are affected by the same filtering rules.

China deploys Internet filtering technology at the Internet backbone level, near international gateway points. Requests for blocked content are routed normally through regional networks but are blocked before the request leaves China’s backbone network and enters the international Internet. All requests are subject to blocking at this location regardless of what ISP is used. Although cyber-café’s and ISPs may implement an additional layer of filtering, at the national level all users are subject to essentially uniform filtering [5].

In contrast, Iran delegates filtering responsibility to ISPs. Each ISP selects its own filtering technology to be used and there are variations in blocked content. The primary ISP, the Telecommunications Company of Iran, uses the commercial product SmartFilter to block access to specific Internet content. SmartFilter’s secret lists are used to block access to pornography and Iran adds additional Web sites to be blocked for political reasons [6]. However, another major ISP, ParsOnline, uses Websense to block access to Internet content. Smaller Iranian ISPs use other filtering products. The result is that there is not uniformity in the content blocked in Iran [7].

Most implementations, especially those at an ISP level, focus on the “block list” approach where access to listed locations are blocked. The blocking may take a number of forms:

- Domain Name Service (DNS) filtering — an ISP makes entries in the DNS servers under its control that prevent requests to those servers for a specific Web site’s fully qualified domain name (found in the requested site’s URL) from resolving to the Web site’s correct IP address.
- IP filtering — an ISP first determines the IP address to which a specific URL resolves. It then makes entries in routing equipment that it controls that will stop all outgoing requests for the specific IP address.
- URL filtering — involves the placement of an additional device, or in some cases the reconfiguration of an existing “router” or other device, in the ISP’s network to (a) reassemble the packets for Internet traffic flowing through its network; (b) read each http Web request; and, (c) if the requested URL in the Web request matches one of the URLs specified in a blocking order, discard or otherwise block the http request [8].

DNS filtering is not a preferred choice for most ISPs. Not only is it easy to circumvent (by accessing an IP address for instance, or using a different DNS server) it is not something that network administrators normally do. DNS servers are used to translate domain names into IP addresses and are updated frequently. Removing DNS records from specific DNS servers involves manual deletion and is not something that occurs in normal network administration.



**Countries such as Iran,
Saudi Arabia, United Arab
Emirates (UAE), Tunisia,
Yemen and Sudan all use
commercial filtering
products developed by
U.S. corporations.**

.....

Blocking by IP is effective (the target site is completely blocked) and no new equipment needs to be purchased. It can be implemented in an instant as all the required technology and expertise is readily available. Existing routers can be configured to block transmissions to designated IP addresses. This feature is usually used to combat spam and viruses but can easily be adapted for Internet filtering. Routers also have built-in functionality for automated rule updates. A network administrator can manage large numbers of routers very easily adding new sites to block on a regular basis. Most ISPs do not have the capacity to filter by URL and the ones that do would need to purchase a significant amount of equipment to implement URL filtering without a significant drop in performance.

However, as the scale of filtering increases, countries begin to adopt the use of commercial technology designed specifically for Internet filtering, most of which is capable of URL filtering. Using commercial products in conjunction with cache servers allows for more precise Internet filtering without a significant loss in performance. Specific URL paths can be easily blocked, allowing all other content on the same site to be accessible. These products are also available with pre-existing categories of URLs that can be blocked or unblocked. This makes the management of block lists much easier and more efficient. The majority of these products are developed and marketed in the U.S. Countries such as Iran, Saudi Arabia, United Arab Emirates (UAE), Tunisia, Yemen and Sudan all use commercial filtering products developed by U.S. corporations [9]. Despite the ability to filter by specific URL, most countries do not make significant use of the technology [10]. Instead most simply block entire domains if any offending content is located.

The implementation of commercial filtering technology at the national level is generally difficult for large ISPs whose networks were not designed to filter [11]. The deployment of commercial filtering technology at the national level is generally restricted to developing countries whose Internet infrastructure can be intentionally designed or adapted to accommodate filtering technology.



Transparency, openness and accountability

The implementation of a filtering strategy is particular to the unique legal, political and technical conditions within a country. This affects not only the decision-making process leading to filtering but the technology used and the targeted content as well. Some countries have specifically designed and centralized backbone Internet connections to facilitate a coordinated, centrally-operated filtering regime while others have implemented *ad hoc* solutions or delegated filtering responsibilities to ISPs. Some are quite transparent about filtering practices, from both a policy and technology standpoint, while others remain closed and secretive.

The way in which the decision to filter is taken is as significant as the technology used. It sets the tone, from the start, as to the amount of transparency and openness there will be in the process and whether or not respect for freedom of speech and expression will factor into the filtering regime. Transparency refers to the level of notification users receive when content is blocked while openness refers to the revealing of what content is blocked, at least in a general descriptive way. When the reason for filtering is clearly articulated the implementation is often more precise than in situations in which such decisions are made behind closed doors.

Governments can legislate the use of filtering technology and order specific content to be blocked. This has been the case in the U.S. when the State of Pennsylvania passed legislation requiring ISPs to block access to sites designated as child pornography. Similar efforts have included government directed partnerships between law enforcement and ISPs and private partnerships between ISPs and non-governmental organizations concerned with the protection of children online [12]. However, most filtering regimes are implemented as a result of vague laws which are open to arbitrary interpretation, ministerial decrees, or obscure “national security” channels.

Most filtering regimes are implemented as a result of vague laws which are open to arbitrary interpretation, ministerial decrees, or obscure “national security” channels.

For example, Iran does not have explicit laws regulating Internet content or requiring the implementation of filtering technology. Rather, Iran uses the country’s Press Law to target specific content. The implementation of filtering is mandated, not by law, but by the Telecommunications Company of Iran (TCI), which is run by the Ministry for Information and Communication Technology (ICT). Filtering is further codified through ISP licensing agreements with the end users in which users agree not to access “non-Islamic” sites [13]. In Myanmar, formerly known as Burma, Internet content is regulated through the “2000 Web Regulations” which prohibits publishing content “detrimental” to state interests [14]. However, there does not appear to be any specific legal requirement to implement filtering or what legal definitions apply to selecting content to be blocked.


India’s Internet filtering regime appears to operate by decree. In September 2003, ISPs in India received a faxed notice from the Ministry of Communications & Information Technology order a specific URL to be blocked. The Mumbai Police Commissioner’s Office also ordered ISPs in India to block a specific Web site [15]. There appears to be jurisdictional and legal uncertainty concerning the implementation of filtering in India.

South Korea’s Internet filtering came as a result of order by the Ministry of Information and Communication (MIC). ISPs in South Korea were instructed to block access to Web sites designated as North Korean propaganda. The filtering action was taken under a Security Law, passed in 1948, to counter the threat of communist influence and infiltration [16]. There appear to be no explicit laws requiring the use of filtering.

In China, the government has established a complex web of regulations for both Internet Service Providers (ISP) and Internet Content Providers (ICP). These regulations manage the delivery of Internet access as well as content within China and define the enforcement policies and mechanisms through which compliance with the regulations is achieved. Although the Ministry of Information Industry (MII) is responsible for the Internet infrastructure, the Ministry of Public Security and the State Secrets Bureau are also involved in the filtering process [17]. While there are explicit regulations that forbid the use of the Internet to incite the “overthrow of the government or socialist system” or “promote feudal superstitions,” it is unclear which specific laws or regulations mandate the use of backbone Internet filtering. Nor is it clear how specific content is chosen to be blocked.

Most countries that filter are unable to publicly answer the following questions: What are the blocking criteria? Is there a review process? What is the policy on collateral blocking? Is there a grievance mechanism? How can designations be changed if there is mis-categorization? How are Internet users informed that they are attempting to access prohibited content?

One measurement of transparency is the behavior that occurs when a user attempts to access filtered content. In some countries a blockpage is used to inform users that they have attempted to access prohibited content. Iran and United Arab Emirates clearly inform users that the content they have requested is blocked. In Saudi Arabia users are presented with a blockpage which states that the requested Web site has been blocked but it also contains a link to a Web form through which users can petition to have the site unblocked [18]. In these cases users are at least aware of the fact that their requested content has been deliberately blocked, and in some cases, are given instructions on how to seek to have content unblocked. The acknowledgment of blocked content allows users to petition to have sites unblocked if there has been a mis-categorization [19]. It also requires governments to justify why a specific site is blocked.



**When a “block” occurs,
the Internet connection
of the user is disrupted.
The connection between
the user and the
requested site is
terminated.**

.....

But some countries obscure the fact that content has been intentionally filtered. In China, for example, the filtering mechanism in place at the Internet backbone level generates an error when prohibited content is requested. When a “block” occurs, the Internet connection of the user is disrupted. The connection between the user and the requested site is terminated [20]. This creates a situation where connections between the two computers are disrupted for a period of time, often up to twenty minutes. This is what is generally referred to as being “banned” or being in the “penalty box.” The disruption does not affect the user’s Internet access, it only applies to connections to the specific IP address which was subject to blocking. This type of filtering produces a network timeout error that does not indicate if or why a site has been blocked. Users are left to wonder why their requested content cannot be accessed.

In Tunisia, a commercial application developed in the U.S. called SmartFilter, marketed by the software company Secure Computing, has been deployed at the national level. This is the same product used in Saudi Arabia and it has the capacity to deliver blockpages to users when prohibited content is requested. Unlike Saudi Arabia, Tunisia uses this blockpage functionality to deliver a false error indication to users. When users attempt to access blocked content, they receive a page that appears to be a “File not found” error page but is in fact a block page designed to deceive users. Often, the use of errors, or in this case false errors, is designed to mask the fact that content is being blocked for political reasons. Saudi Arabia, for example, blocks little political content and focuses on pornography and gambling sites. Citing cultural reasons, Saudi Arabia is quite open about filtering. On the other hand, Tunisia is quite closed about what type of content is filtered. Tunisia targets a significant amount of political content and has been the object of condemnation by international human rights organizations. The use of an “error page” rather than a block page may be an attempt to deflect criticism, allowing the authorities to claim that they are not censoring Internet content [21].

Uzbekistan uses similar deceptive practices. In Uzbekistan, some ISPs provide a blockpage to users indicating that the requested content has been blocked because it is pornographic. However, some political Web sites are blocked in this way even though they do not contain any pornography. For key political sites, Uzbekistan uses re-direction as a mechanism of filtering. Instead of viewing the requested content or being delivered a blockpage, users in Uzbekistan are redirected to innocuous sites. In some cases, users who attempt to reach a specific page on a site are redirected back to the site's front page. This renders all "deep links" inaccessible, although the front page of the site is accessible [22]. This practice also disguises filtering, since the Web site itself appears available, but sensitive content in that site is blocked.

Deceptive practices indicate the lack of transparency with regard to filtering as well as a determined effort to avoid accountability. Countries seek to intentionally deceive users with regard to their filtering practices and have no mechanisms for redress or accountability. Generally, countries engage in deceptive filtering practices when the content targeted for blocking is political. Unable to justify the reason for blocking political content, countries choose to obscure or deny the fact that such content is in fact targeted.

Many countries implement filtering in order to block pornographic content. Most countries use commercial filtering lists to target this content and have achieved reasonable levels of success. Saudi Arabia, UAE and Iran blocked 100 percent of all pornographic sites tested by the OpenNet Initiative. All three use the commercial product SmartFilter. Uzbekistan's UzScinet blocked pornographic content at a rate of 89 percent. While China has been cracking down on domestically produced pornography, China blocked pornography at a rate of only 39 percent. Of all the topics tested by the OpenNet Initiative, pornography is blocked with the highest overall percentage rates. Pornography is not language-specific and thus commercial enterprises create targeted lists that are used by countries worldwide.



In order to counter attempts to bypass the filtering restrictions, countries frequently heavily block public anonymizer and circumvention sites.

There is a sizable breadth of general, non-pornographic content targeted for Internet filtering in most countries. As part of general testing, the OpenNet Initiative tests a "global list" of Web sites organized into 31 high-level categories. The results are used to assess general content areas that countries may wish to target for filtering. In order to counter attempts to bypass the filtering restrictions, countries frequently heavily block public anonymizer and circumvention sites. Anonymizers are sites that allow users to browse through the site itself, thus bypassing Internet filtering restrictions. Anonymizer Web sites contain software that retrieves a requested page on behalf of a user and thereby evades filtering as the user never directly connects to the blocked site. Other key topic areas that are targeted for filtering include gambling sites, provocative attire, hate speech, and non-pornographic gay and lesbian sites. Countries that use commercial filtering software generally block these general categories with higher percentages of effectiveness than do countries which produce their own blocklists.

Most countries that filter the Internet target content that is specific to the country itself and is in the local language. The focus is on "high impact" Web sites or keywords that contain content that governments consider to be sensitive or taboo. These Web sites generally include domestic human rights organizations, independent media, opposition groups or political parties, and religious conversion or spiritual groups. Sites that contain content opposed to or dissenting from the views of the current government are most often the targets of filtering. The control over information begins to move from filtering into overt political censorship.

China blocks access to Web sites containing content related to Taiwanese and Tibetan independence, Falun Gong, the Dalai Lama, Tiananmen Square, and opposition political movements. The filtering regime in China operates with a lack of transparency. China rarely admits to filtering the Internet. There is no public list of banned sites and no mechanism for citizens to petition to have a site unblocked [23].

Iran blocks access to Web sites of banned political parties, the monarchy [24], independent media and blogs. Iran also uses commercial filtering software to block access to pornography. While Iran has publicly acknowledged filtering the Internet and uses blockpages to inform users that content is blocked, the list of blocked sites and the specific criteria used to determine which sites to block are not public. There is also no mechanism for citizens to petition to have a site unblocked [25].

Uzbekistan blocks access to the Web sites of banned Islamic movements, independent media, NGOs and Web sites critical of the government's human rights record, and UzSciNet blocks access to pornography. Political content is blocked deceptively and there is no mechanism for citizens to petition to have a site unblocked [26].

When targeting political content, filtering is implemented in an unaccountable and non-transparent way. States are increasingly using Internet filtering to control the environment of political speech in fundamental opposition to civil liberties, freedom of speech, and free expression. The consequences of political filtering directly impact democratic practices and can be considered a violation of human rights.

Unintended consequences

Filtering systems suffer two inherent flaws: over-blocking and under-blocking. Not only do filtering technologies often block access to content that is unrelated to banned topics, they often do not block access to all content intended to be blocked. In effect, there are two types of lists used for filtering: government lists and commercial lists. Commercial lists consist of categorized domains and URLs targeting content such as pornography, gambling, and, recently, human rights groups [27]. Filtering technology manufacturers are not transparent about the process through which URLs are collected and added to block lists. Many claim that each URL is reviewed by people, rather than software tools, but the prevalence of inaccuracy in filtering lists casts doubt on this claim. Most lists are created through a combination of automated collection and limited human review [28].

**In effect, U.S.
corporations are in a
position to determine
what millions of citizens
can and cannot view on
the Internet.**

Commercial filtering lists are the intellectual property of their manufacturers and are not made public. Despite the fact that some filtering software manufacturers offer online URL checkers — sites that allow one to check how a particular URL is categorized by the filtering software — the block lists as a whole are secret and unavailable for independent scrutiny and analysis. This inherent flaw is exacerbated when entire countries rely on such commercial filtering programs. For example, Saudi Arabia was condemned by human rights organizations for blocking access to non-pornographic gay and lesbian sites. After learning about the blocked sites, the Saudi authorities promptly removed the blocking [29]. Saudi Arabia never intended to block access to these sites. These sites were likely misclassified by the commercial filtering product, SmartFilter, that Saudi Arabia implemented at the national level. In effect, U.S. corporations are in a position to determine what millions of citizens can and cannot view on the Internet. Even the countries implementing filtering products do not know for certain what is in fact being blocked.

Government lists generally consist of sites that highlight corruption or oppose the regime in power, report on human rights abuses, or publish the writings of independent journalists. Government lists are generally added to commercial filtering lists. There is considerable variation in the reported centralization of filtering lists as well as governments' capacities to update the lists. For example, in cases where the government relies on individual ISPs to implement filtering there is often considerable variations in the actual content filtered. Moreover, many

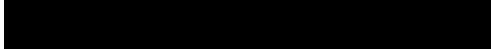
countries that filter continue to block defunct and expired Web sites which indicates that content is rarely reviewed once blocked [30]. These factors are affected by the legal — or lack of legal — status regarding the filtering regime in a country as well as the technology being used to filter.

In addition to the unintended consequences of using commercial filtering products there are additional consequences that affect *ad hoc* filtering implementations. Countries new to filtering will generally start blocking by IP address before moving on to more expensive commercial filtering solutions. ISPs must often respond quickly and effectively to blocking orders from the government or national security/intelligence services. So they block what was requested in the cheapest way using technology already integrated into their normal network environment: filtering by IP address. Routers have the built-in capacity to block IP addresses. When an IP address is blocked, all sites hosted on that server will be blocked. (Many Web hosting companies employ “virtual hosting,” a term that refers to the way in which many thousands of individual Web sites can be hosted on a server at a single IP address.) When an IP address is blocked, there is a significant chance that many unrelated Web sites will be blocked in the process.

For example, South Korea has an advanced Internet infrastructure. Yet when implementing Internet filtering, South Korean ISPs have chosen to block by IP address. As a result, while trying to block 31 Web sites, they actually blocked 3,167 unrelated domain names hosted on the same servers as the sites they intended to block [31].

This type of over blocking also occurred in India. The Ministry of Communications & Information Technology in India ordered ISPs to block access to a specific Yahoo! Group named *kynhun*. The ISPs were unable to block the specific URL, presumably due to a lack of specialized technology, so instead they blocked access to the entire groups.yahoo.com domain by configuring their routers to block access to the specific Yahoo! Groups IP address. This caused many thousands of Yahoo! Groups to be inaccessible to Internet users in India [32].

Morocco recently introduced Internet filtering and blocked the IP addresses of the following Web sites that promote independence for Western Sahara: <http://www.arso.org/>, <http://cahiersdusahara.com/>, <http://wsahara.net/> and <http://www.spsrasd.info/> [33]. The site <http://www.afapredesa.org/> is also blocked. In blocking these five sites Morocco is actually blocking at least 2,287 domains [34].



**Often, those
implementing filtering
are unaware of the
consequences that the
mechanism of filtering
can have.**

.....


A major ISP in Canada, Telus, ran into similar trouble when attempting to block a site set-up by workers during a strike action with the Telecommunications Workers Union. Telus blocked the Union site’s IP address, causing more than 600 other, non-related Web sites to be blocked for all Telus subscribers in the process [35].

Often, those implementing filtering are unaware of the consequences that the mechanism of filtering can have. They most likely do not consider overblocking due to virtual hosting, or consider it acceptable collateral damage. Indiscriminate blocking of IP addresses can interfere with e-commerce in addition to normal Internet traffic and is particularly problematic because technology does exist that avoids this type of collateral filtering. This filtering practice runs in direct opposition to the design of the Internet, for it unilaterally interferes with and disrupts legitimate transfers of information. This collateral filtering seriously affects freedom of speech and expression online and may in fact be illegal in locations where filtering rules are clearly articulated.

Mission creep

Filtering is perceived as an inexpensive technical solution to the challenges posed by the ease of access to information on the Internet. Regardless of the initial reason for implementing Internet filtering, there is increasing pressure to expand its use once the filtering infrastructure is in place. In 2004, Thailand began the process of implementing Internet filtering. Unlike many countries, the process was largely transparent. Under the auspices of the Thai Information and Communications Technology Ministry numerous officials, child protection advocates and computer scientists met to determine what content should be filtered. While agreement was reached on the filtering of “extreme pornography or violence” there was considerable debate on targeting other content [36]. Despite the lack of agreement, the Communications Authority of Thailand (CAT), the entity which creates the blocklists distributed to ISPs, included sites that are critical of the Royal Family [37]. Moreover, at least one unofficial block, a site detailing government corruption, has been identified [38]. This blocked site does not appear on the CAT’s blocklist. In 2005, CAT ordered additional anti-corruption sites, Thai-insider.com and FM9225.com, to be blocked [39]. Filtering, ostensibly for the purposes of blocking pornography, now includes content targeted for political reasons.

Malaysia has approved recommendations to restrict access to pornography. Schools and libraries are now required to install filtering software. Other measures to be introduced require ISPs to provide optional filtering services, a complaint centre where Internet users can report obscene content, and awareness campaigns against pornography [40]. But some are questioning the move, suggesting that the implementation of a filtering infrastructure for pornography can be easily configured to block political content [41]. In addition to the overblocking associated with filtering software, Malaysia could easily add sites to the block lists for political reasons once the filtering infrastructure is in place.



**Once a national filtering
system is in place,
governments may be
tempted to use it as a
tool of political
censorship or as a
technological “quick fix”
to problems that stem
from larger social and
political issues.**

.....

Once a national filtering system is in place, governments may be tempted to use it as a tool of political censorship or as a technological “quick fix” to problems that stem from larger social and political issues.

Terrorism has long been an object of media attention, the subject of study by academics and a matter of focus for politicians, but never has the world’s attention been so heavily focused on this issue as it is now. This focus has not been limited to conventional methods of terrorism; it has extended into the realm of cyberspace. While much of the attention has focused on vulnerabilities in critical infrastructure nodes, the use of the Internet and computer technology by traditional terrorist organizations for organizational and logistical purposes, data collection, communications and propaganda is also becoming a concern [42].

While some may suggest filtering as a solution to the problem of online terrorism, its effectiveness as a means of disrupting communications between networked groups is limited. Filtering is primarily restricted to Web-based communications and largely ignores alternative means of communications such as e-mail, instant messaging, peer-to-peer technologies, and VoIP. Therefore, it does not disrupt communications between various members within the terrorist organization. Countries may be able to filter casual or inadvertent access to Web sites associated with or promoting various terrorist groups but this will not significantly impact those determined to view this content.

In Egypt the Web site <http://www.ikhwanonline.com>, the official Web site of the Muslim Brotherhood, is blocked. Despite this blocking, Muslim Brotherhood candidates, running as independents, won a considerable number of seat in Egypt’s 2005 parliamentary election cementing their position as the main opposition to the

ruling National Democratic Party [43]. In order to counter the blocking, the Muslim Brotherhood has changed their Web server's IP address several times and now operate a mirror site that is not blocked. Moreover, Human Rights Watch reports that the Muslim Brotherhood is "now using third-party sites they do not officially endorse — public bulletin boards, chat rooms, and so on — to coordinate their activities" [44].

There are numerous circumvention technologies, also known as anonymizers, available that allow users to access filtering content. These anonymizers operate by allowing users to request content through computers located in unfiltered locations. The filtered user connects to a computer in an unfiltered country that is configured to retrieve the requested content and transmit it back to the users in the filtered location. There is no direct connection between the user and the filtered Web site. There is a wide range of circumvention technologies available ranging from simple scripts to complex peer-to-peer protocols [45].

The most commonly used circumvention technology is a Web-based circumventor. Essentially, a Web-based circumventor is a Web site that has a standard Web form through which users can submit requests for filtered URLs. This Web site has a specially designed script that fetches the request page for the user and re-writes all the links in the page to point back through the Web-based circumventor. Using this technology a user can seamlessly browse the Internet without being subjected to Internet filtering.

This type of circumvention technology is being used by Internet users in China to bypass the filtering restrictions in that country [46]. The U.S. Government has sponsored similar technology, albeit poorly designed, for use by Iranian Internet users [47]. While many users may be unwilling to use circumvention technology for fear of reprisal, determined Internet users will always be able to use this type of technology to bypass filtering restrictions.


Although governments and commercial filtering manufacturers actively target public anonymity and circumvention sites, they are unable to effectively counter distributed, private circumvention strategies.




Conclusion

Despite the Internet's decentralized architecture, states have implemented both legal and technical mechanisms to control their citizens' access to and publication of information on the Internet. Combining low-tech and high-tech solutions, states have created a complex regulatory framework that is combined with Internet filtering and monitoring. Controls are placed at multiple levels of access including educational facilities and cyber-café's as well as at the national level. Filtering is implemented at locations such as ISPs and at the Internet backbone and international gateways.

Procedurally, filtering is most often imposed through interpretations of vague laws and regulations, by ministerial decree, or through unaccountable national security channels. There is little transparency regarding the selection of sites to block and citizens rarely have any recourse to petition to have a site unblocked. While some states are open about the fact that filtering has been implemented — by showing users a blockpage when attempting to access filtered content — some deceive their citizens by masquerading filtering as a generic network error or by redirecting users to innocuous content. Often, these deceptive practices are used to target political content such as human rights groups and independent media.



**All too often,
governments cannot
resist extending filtering
to silence criticism and
control political speech
online.**



Filtering technology cannot block all content that governments intend to block and it often blocks content that

was never intended to be blocked. This creates cases of collateral filtering which have serious implications for both freedom of speech as well as the normal functioning of the Internet. For example, collateral blocking could impact e-commerce in a negative way. However, states seem resigned to filtering's fundamental flaws.

Filtering is seen as a technical "quick fix" to much broader social and political problems. This results in cases of "mission creep" where the initial reason for implementing filtering is extended to other content areas. Often states that implement filtering to target pornographic content will extend this capability to block content for political reasons as well. All too often, governments cannot resist extending filtering to silence criticism and control political speech online.


Internet filtering alone, especially when restricted to Web-based filtering, cannot completely control a person determined to access blocked content. At best, it prevents casual or inadvertent access to designated Web sites. Filtering is rarely applied to peer-to-peer, instant messaging and file sharing protocols. Moreover, filtering systems can be easily circumvented through the use of Web-based circumvention systems and anonymous communications systems. Despite the efforts of governments and commercial filtering manufacturers to block anonymizers and circumventors many public circumvention systems remain unblocked. Private circumvention systems are unblockable and development efforts are underway to create attack resistant public circumvention systems.



Filtering is not a communications disruption tool. It does not disrupt terrorists' use of the Internet. It does not protect against cyberterrorism.

.....

Filtering is not a communications disruption tool. It does not disrupt terrorists' use of the Internet. It does not protect against cyberterrorism.

National filtering is implemented to impose information control on populations within a given geographic space. There are significant transparency and accountability concerns regarding the decision to implement Internet filtering and the selection of targeted content. Often, those implementing filtering are unaware of the consequences that the mechanism of filtering can have. While easily circumvented, Internet filtering inflicts "collateral damage" that represents a significant threat to transparent and democratic practices. 

About the author

Nart Villeneuve is the Director of Technical Research at the Citizen Lab, an interdisciplinary laboratory based at the Munk Centre for International Studies at the University of Toronto. As both a software developer and academic, he is currently working with the OpenNet Initiative (ONI), documenting Internet content filtering and surveillance practices worldwide. He has also been working on documenting and evaluating existing circumvention technology as well as developing circumvention technology.

Blog: <http://ice.citizenlab.org>

E-mail: nart [at] citizenlab [dot] org

Notes

1. Voice-over-Internet-Protocol is technology that allows voice communications, such as phone calls, to be made over the Internet.

2. For content that is hosted domestically, takedown and removal are preferred methods. Since the servers are hosted domestically, government can just authorize ISPs to remove offending content.
3. Countries may use keyword filtering, as China does, to broaden the content that is filtered, however, this is generally restricted to keywords in URLs. URLs that contain offending content but do not have such keywords in the URL path will not be blocked.
4. Ronald Deibert and Nart Villeneuve, 2004. "Firewalls and power: An overview of global state censorship of the Internet," In: Andrew Murray and Mathias Klang (editors). *Human rights in the digital age*. London: GlassHouse.
5. OpenNet Initiative, 2005. "Internet filtering in China," at <http://www.opennetinitiative.net/studies/china/>, accessed 29 December 2005.
6. OpenNet Initiative, 2005. "Internet filtering in Iran," at <http://www.opennetinitiative.net/studies/iran/>, accessed 29 December 2005.
7. The author conducted tests on ParsOnline and other smaller ISPs which indicated that various products, including Websense, are in use in Iran.
8. DNS is an Internet service that translates domain names into IP addresses. An IP address is a numeric designation used for routing on a TCP/IP network. A URL (Uniform Resource Locator) is an address used to access content on the World Wide Web.
- J. Dubios, 2004. "Memorandum Center for Democracy and Technology v. Attorney General of the Commonwealth of Pennsylvania," at <http://www.cdt.org/speech/pennwebblock/20040910memorandum.pdf>, accessed 29 December 2005.
9. The author has conducted tests confirming the use of commercial filtering products in all these countries. The use of SmartFilter has been documented in OpenNet Initiative reports on as Iran, Saudi Arabia, and UAE. For Tunisia see: IFEX Tunisia Monitoring Group, 2005. "Tunisia: Freedom of Expression under Siege," at <http://www.ifex.org/download/en/FreedomofExpressionunderSiege.doc>, accessed 29 December 2005.
10. There are some significant exceptions. Saudi Arabia, for example, the domain [amnesty-usa.org](http://www.amnesty-usa.org) is accessible, but a specific URL (http://www.amnesty-usa.org/countries/saudi_arabia/morenewsandreports.html) containing content critical of Saudi Arabia is blocked.
11. Major ISPs in the U.S. including AOL, Verizon, and WorldCom testified that they were unable to implement URL filtering on their networks, citing significant expense and possible negative impact on their quality of service. See J. Dubios, 2004. "Memorandum Center for Democracy and Technology v. Attorney General of the Commonwealth of Pennsylvania," at <http://www.cdt.org/speech/pennwebblock/20040910memorandum.pdf>, accessed 29 December 2005.
12. In Norway, Telenor and KRIPOS, the Norwegian National Criminal Investigation Service, have introduced a new filter system. In the U.K., British Telecom, blocks access to child pornography sites compiled by the Internet Watch Foundation (IWF). Telenor, 2004. "Telenor and KRIPOS introduce Internet child pornography filter," at http://press.telenor.com/PR/200409/961319_5.html, accessed 29 December 2005 and Martin Bright, 2004. "BT puts block on child porn sites," *The Guardian*, at <http://www.guardian.co.uk/online/news/0,12597,1232506,00.html>, accessed 29 December 2005.
13. OpenNet Initiative, 2005. "Internet filtering in Iran," at <http://www.opennetinitiative.net/studies/iran/>, accessed 29 December 2005.
14. OpenNet Initiative, 2005. "Internet filtering in Burma," at <http://opennetinitiative.net/studies/burma/>, accessed 29 December 2005.
15. OpenNet Initiative, 2004. "Internet content filtering in India: Variations in compliance and accuracy," at <http://www.opennetinitiative.net/bulletins/003/>, accessed 29 December 2005; and, Priya Ganapati, 2004. "Mumbai police gag hinduunity.org," *Rediff.com*, at <http://us.rediff.com/news/2004/may/26hindu.htm>, accessed 29 December 2005.

16. OpenNet Initiative, 2005. "Collateral blocking: Filtering by South Korean government of pro-North Korean Web sites," at <http://www.opennetinitiative.net/bulletins/009/>, accessed 29 December 2005.
17. OpenNet Initiative, 2005. "Internet filtering in China," at <http://www.opennetinitiative.net/studies/china/>, accessed 29 December 2005.
18. The blockpage in Saudi Arabia also contains a link to a form to request that a site be added to the blocking list.
19. For example, the Websense filtering software categorized Microsoft's download page as a "marijuana" site. See John Leyden, 2005. "Websense makes hash of MS classification," *The Register*, at http://www.theregister.co.uk/2005/11/04/ms_websense_hash/, accessed 29 December 2005.
20. For a more detailed technical explanation of this process see OpenNet Initiative, "Google Search & Cache Filtering Behind China's Great Firewall," at <http://www.opennetinitiative.net/bulletins/006/>, accessed 29 December 2005; and, Nart Villeneuve, 2005. "Censorship is In the Router," at <http://ice.citizenlab.org/?p=113>, accessed 29 December 2005.
21. IFEX Tunisia Monitoring Group, 2005. "Tunisia: Freedom of expression under siege," at <http://www.ifex.org/download/en/FreedomofExpressionunderSiege.doc>, accessed 29 December 2005.
22. OpenNet Initiative, 2006. "Internet filtering in Uzbekistan," in press, <http://www.opennetinitiative.net/>.
23. Blocked sites include <http://www.amnesty.org>, <http://www.president.gov.tw> and <http://news.bbc.co.uk>. See OpenNet Initiative, 2005. "Internet filtering in China," at <http://www.opennetinitiative.net/studies/china/>, accessed 29 December 2005.
24. The Shah of Iran was overthrown in the 1979 Islamic Revolution.
25. Blocked sites include <http://www.cpiran.org/>, <http://www.hoder.com> and <http://www.iran-e-sabz.org>. See OpenNet Initiative, 2005. "Internet filtering in Iran," at <http://www.opennetinitiative.net/studies/iran/>, accessed 29 December 2005.
26. Blocked sites include <http://www.muslimuzbekistan.com>, <http://www.stopdictatorkarimov.com> and <http://www.soros.org>. See OpenNet Initiative, 2006. "Internet filtering in Uzbekistan," in press, <http://www.opennetinitiative.net/>.
27. Both SmartFilter and Websense have categories that target human rights groups: Non-Profit Organizations/Advocacy Groups (<http://www.securecomputing.com/index.cfm?skey=86#np>) and Service and Philanthropic Organizations (<http://www.websense.com/global/en/SupportAndKB/SiteLookup/>)
28. See the promotional materials for SmartFilter: <http://www.securecomputing.com/index.cfm?skey=86>.
29. See OpenNet Initiative, 2004. "OpenNet Initiative: Bulletin 002" at <http://opennetinitiative.net/bulletins/002/>, accessed 29 December 2005; and, Reporters Without Borders, 2004. "Ban lifted on two gay websites," at http://www.rsf.org/article.php3?id_article=9586, accessed 29 December 2005.
30. For example, in Tunisia, the Web site of the Movement of Democratic Socialists (<http://www.mdstunisie.org>) is blocked even though it has expired. See Elijah Zarwan, 2005. "False Freedom: Online Censorship in the Middle East and North Africa," *Human Rights Watch*, at <http://hrw.org/reports/2005/mena1105/index.htm>, accessed 29 December 2005.
31. OpenNet Initiative, 2005. "Collateral Blocking: Filtering by South Korean Government of Pro-North Korean Websites," at <http://www.opennetinitiative.net/bulletins/009/>, accessed 29 December 2005.
32. OpenNet Initiative, 2004. "Internet Content Filtering in India: Variations in Compliance and Accuracy," at <http://www.opennetinitiative.net/bulletins/003/>, accessed 29 December 2005.
33. Reporters Without Borders, 2005. "Access to Sahrawi sites blocked within Morocco," at http://www.rsf.org/article.php3?id_article=15809, accessed 29 December 2005.

34. Nart Villeneuve, 2005. "Internet filtering in Morocco," at <http://ice.citizenlab.org/?p=165>, accessed 29 December 2005..
35. OpenNet Initiative, 2005. "Telus Blocks Consumer Access to Labour Union Web Site and Filters an Additional 766 Unrelated Sites," at <http://www.opennetinitiative.net/bulletins/010/>, accessed 29 December 2005.
36. *Bangkok Post*, 2003. "Thai Internet censors can't agree what to ban," at http://www.thaivisa.com/index.php?514&backPID=10&tt_news=523, accessed 29 December 2005.
37. *Bangkok Post*, 2003. "Govt forces ISPs to block 'inappropriate' Web sites," at http://www.thaivisa.com/index.php?514&backPID=514&tt_news=434, accessed 29 December 2005.
38. Jeffrey Race, 2004. "Censoring the Internet in Thailand," at http://www.camblab.com/nugget/block/block_01.htm, accessed 29 December 2005.
39. See Web site censorship in Thailand, at <http://2bangkok.com/blocked.shtml>, accessed 29 December 2005; and, Committee to Protect Journalists, at http://www.cpj.org/cases05/asia_cases05/thai.html, accessed 29 December 2005.
40. See Edwin Yapp, 2005. "Slamming door on porn opens others," at <http://star-techcentral.com/tech/story.asp?file=/2005/6/21/technology/11282315&sec=technology>, accessed 29 December 2005; and, *News24*, 2005. "Porn sites must be blocked," at http://www.news24.com/News24/World/News/0,,2-10-1462_1721610,00.html, accessed 29 December 2005.
41. Arbibi Ashoy, 2005. "Where will 'block porn sites' move lead to?," at <http://www.malaysiakini.com/letters/37126>, accessed 29 December 2005.
42. Timothy L. Thomas, 2003. "Al Qaeda and the Internet: The danger of cyberplanning," *Parameters*, volume 33, at <http://carlisle-www.army.mil/usawc/Parameters/03spring/thomas.pdf>, accessed 29 December 2005.
43. Michael Slackman, 2005. "Muslim Brotherhood cements its leadership of Egyptian opposition," *International Herald Tribune*, at <http://www.iht.com/articles/2005/11/27/news/egypt.php>, accessed 29 December 2005.
44. Elijah Zarwan, 2005. "False Freedom: Online Censorship in the Middle East and North Africa," *Human Rights Watch*, at <http://hrw.org/reports/2005/mena1105/index.htm>, accessed 29 December 2005.
45. Nart Villeneuve, 2005. "Choosing Circumvention: Technical Ways To Get Around Censorship," *Reporters Without Borders, Handbook for Bloggers and Cyber-dissidents*, at http://www.rsf.org/rubrique.php3?id_rubrique=542, accessed 29 December 2005.
46. Bill Xia, 2002. "Statement of Bill Xia, China's Cyber-Wall: Can technology break through?" at <http://cecc.gov/pages/roundtables/110402/xiaStatement.php>, accessed 29 December 2005.
47. OpenNet Initiative, 2004. "Unintended Risks and Consequences of Circumvention Technologies: The IBB's Anonymizer Service in Iran," at <http://opennetinitiative.net/advisories/001/>, accessed 29 December 2005.

Editorial history

Paper received 29 December 2005; accepted 4 January 2006.

[Contents](#) [Index](#)



This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 2.5 License](http://creativecommons.org/licenses/by-nc-sa/2.5/).

The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace by Nart Villeneuve

First Monday, volume 11, number 1 (January 2006),

URL: http://firstmonday.org/issues/issue11_1/villeneuve/index.html