Local Nets: Filtering and the Internet Governance Problem

John G. Palfrey, Jr.[†]
(Chapter in Jack Balkin et al., *The Global Flow of Information)*
September, 2005

Introduction.

In dozens of nations around the world, the state takes part in censoring what their citizens can see and do on the Internet. This practice is increasingly widespread, with extensive filtering regimes in place in China, Iran, Burma (Myanmar), and Uzbekistan, among many other countries. Censorship using technological filters is often coupled with harsh laws related to what the press can publish, opaque surveillance practices, and severe penalties for people who break the state's rules of using the Internet.

At the same time as Internet censorship grows, heads of state and their representatives have been gathering every two years for a World Summit on the Information Society. The widespread practice of blocking citizens from accessing certain information on the Internet from within a given state offers a point of engagement for the Internet governance debate that takes place at this summit. The World Summit on Information Society's planners, the members of the United Nations ICT Task Force, the members of the United Nations' Working Group on Internet Governance and others at the center of the Internet governance debate should help to establish a set of principles and best practices related to Internet filtering.

The Internet filtering problem, on one level, is an unattractive candidate for the Internet governance decision-makers to take up. Diplomatic niceties make hard conversations about divisive issues unpleasant. A serious discussion of Internet filtering would dredge

[†] John Palfrey is the Executive Director of the Berkman Center for Internet & Society and a Lecturer on Law at Harvard Law School. This chapter is based in part on a draft report on Internet filtering worldwide, co-authored with Jonathan Zittrain, the Jack N. and Lillian R. Berkman Assistant Professor for Entrepreneurial Legal Studies at Harvard Law School. Palfrey and Zittrain are co-principal investigators of the OpenNet Initiative, which is a collaborative research effort between the University of Toronto (Prof. Ron Deibert, principal investigator, and Nart Villeneuve, director of technology), the University of Cambridge (Rafal Rohozinski, principal investigator), and Harvard Law School (where they are joined by Berkman fellows Derek Bambauer and Jeffrey Engerman).

up thorny topics like free expression, privacy, national security, international enforcement, and state sovereignty – issues on which states are likely to disagree vehemently. But in so doing, the Internet governance debate might take on new life. It could focus discussion on the core problems related to the divergence of views among states as to what a "good" Internet looks like. It would put in relief the jurisdictional issues related to every country in the world sharing a single, unitary, public network of networks, far more powerful than any such network that has come before, with the power to bring people together and to divide them – while also acknowledging the fact that states can and do exert power over what their citizens do on this network. It would prompt an examination of whether any single set of rules might serve to address concerns related to content on the Internet. And, in the process, it would encourage states to come clean about the lengths they are willing to go to block their citizens from accessing information online. At best, such a discussion would bring the issue of state-based Internet censorship into the spotlight and might, in the process, lead some states to reform their Internet filtering practices so as to become more open and transparent.

1.0 The Internet Governance Debate.

No one is quite sure what the Internet governance debate is all about, exactly. Since the round of preparatory conferences leading up to the first meeting of the World Summit on Information Society (WSIS) in December, 2003, the net has buzzed with a mixture of fear, mistrust, conspiracy theories, posturing, and horse-trading. Most people who have involved themselves in the law and policy in this area are certain that Internet Governance is surely quite important. But points of orientation – handholds – in the debate are elusive, beyond the set of abstract principles set forth at the end of the first WSIS gathering. Consider that the full efforts of the United Nations' Working Group on Internet Governance, ably chaired by veteran Swiss diplomat Markus Kummer, have been oriented toward coming up with a *definition* of Internet governance – a year and a half after the first WSIS meeting.

The problem is *not* that there is a shortage of candidates worthy of the attention of the many capable minds focused on Internet governance.[1] Not surprisingly, the primary lightening rod off the bat is the beleaguered Internet Corporation for Assigned Names and Numbers (ICANN). While deeply flawed from a structural perspective and still much in need of overhaul, ICANN occupies an arcane bit of turf – essentially, the port allocation business – that matters very little to most users of the Internet.[2] Possibilities for consideration other than ICANN reform, each more important to the end users of the Internet and their sovereigns, include a fund for developing countries to build Internet infrastructure, the quandary of what to do about spam, and even a cluster of problems ordinarily considered intellectual property concerns.

Internet filtering is a better candidate for consideration and focus by the world's heads of state. While it raises a wide array of issues, a discussion of Internet filtering would hone in on whether states actually want their citizens to have full access to the Internet or not. It would help guide a public conversation about what is truly most important about having access to the Internet and the extent to which states place a premium, if at all, on the global flow of information. Without collective action, the Internet will likely continue to become balkanized into a series of local networks, each governed by local laws, technologies, markets, and norms. As Prof. Jonathan Zittrain has noted, we may be headed toward a localized version of the Internet, governed in each instance by local laws.[3] If such a version of the Internet is inevitably part of our future, perhaps there is a way to embrace it that can preserve elements of the network that are the most important. And if the free and open, truly "world wide" web is what we are after, intervention may be needed to preserve it.

---

[1] The International Telecommunication Union, the official host of WSIS in Geneva, has held several events designed to refine the debate further. Through these events, the ITU has convinced dozens of observers to publish what comprises an extensive body of work on this topic on the ITU web site. In addition, long-time experts in this field, such as Prof. Milton Mueller of Syracuse and others, have constructed helpful models to structure the conversation. For pointers to further information of this general nature, please see http://www.netdialogue.org, a joint project of Harvard Law School and Stanford Law School.

[2] Witness the abysmal turnout for ICANN's election of 2000, in which a free and open election for five ICANN directors attracted fewer than 100,000 votes globally.

[3] Jonathan Zittrain, *Be Careful What You Ask For, in* WHO RULES THE NET? INTERNET GOVERNANCE AND JURISDICTION, 13 – 30 (Adam Thierer et al. eds., 2003).

2.0 The Internet Filtering Problem.

The fact that extensive Internet filtering occurs around the world is well-documented. Through a collaborative research effort called the OpenNet Initiative,[4] the Citizen Lab at the University of Toronto, the Berkman Center at Harvard Law School, and the Advanced Network Research Group at the University of Cambridge are together comparing the Internet filtering practices of a series of states in a systematic, methodologically rigorous fashion. A primary goal of this research is to reach useful substantive conclusions about the nature and extent of Internet filtering in a number of states and to compare practices across regions of the world. The OpenNet Initiative has released extensive reports that document and provide context for Internet filtering, previously reported anecdotally, in each of the dozen or so countries that we have studied closely. Our reports released to date have focused on states in the Middle East, East Asia, and Central Asia, where the world's most extensive filtering takes place.

Filtering implementations (and their respective scopes and levels of effectiveness) vary widely among the countries we have studied. China, as documented in a number of studies and supported by the OpenNet Initiative's findings, institutes by far the most intricate filtering regime in the world, with blocking occurring at multiple levels of the network and covering content that spans a wide range of topic areas. Though its filtering program is widely discussed, Singapore, by contrast, blocks access to only a handful of sites, each pornographic in nature. Most other states that we are studying implement filtering regimes that fall between the poles of China and Singapore, each which significant variation from one to the next. These filtering regimes can be understood only in the political, legal, religious and social context in which they arise.

Internet filtering occurs in different ways in different parts of the world. Some states implement a software application developed by one of a small handful of United States-based technology providers. Burma, in the first incarnation of its filtering regime, has used an open source product for filtering, called DansGuardian. Others rely less on

[4] http://www.opennetinitiative.net/

technology solutions and more on "soft controls." Sometimes the filtering regime is supported explicitly by the state's legal code; in other cases, the filtering regime is carried out through a national security authority, or just presumed to be permissible. The content blocked spans a wide range of social, religious, and political information. Our studies have combined a review of whether individual citizens could access sites in a "global basket" of bellwether sites to test in every jurisdiction across a variety of sensitive areas – akin to a stock index sorted by sector – as well as a list of Web sites likely to be sensitive in some categories only in some countries.

2.1 Extent, Character, and Locus of Filtering.

Preliminary results from our studies and the work of others in this field, such as Reporters Sans Frontières, show that Internet filtering is not – at least not yet – apparently pervasive in the world, but that those states that do filter have established a network of laws and technical measures to carry out substantial amounts of filtering that could allow the practice to become further embedded in their political and cultural environments. Web content is constantly changing, of course, and no state we have yet studied, even China, seems able to carry out its Web filtering in a comprehensive manner, *i.e.* consistently blocking access to a range of sites meeting specified criteria. China appears to be the most nimble at responding to the shifting Web, likely reflecting a devotion of the most resources to the filtering enterprise.

As our colleagues at the University of Toronto have shown, a state wishing to filter its citizens' access to the Internet has several initial options: DNS filtering, IP filtering, or URL filtering.[5] Most states with advanced filtering regimes implement URL filtering, as it can avoid even more drastic overfiltering or underfiltering situations presented by the other choices and discussed below ("Filtering and Overbreadth").[6] To implement URL filtering, a state must first identify where to place the filters; if the state directly controls

[5] http://ice.citizenlab.org/index.php?p=78

[6] For instance, IP filtering forces the choice of blocking all sites sharing an IP address. A recent ONI bulletin found over 3,000 web sites blocked in an attempt to prevent access to only 31. (see http://www.opennetinitiative.net/bulletins/009/). DNS blocking requires an entire domain and all subdomains to be either wholly blocked or wholly unblocked. (http://ice.citizenlab.org/index.php?p=78)

the ISP(s), the answer is clear. Otherwise, the state may require private or semi-private ISPs to implement the blocking as part of their service. The technical complexities presented by URL become non-trivial as the number of users grows to millions rather than tens of thousands. Some states appear to have limited overall access to the Internet in order to keep URL filtering manageable. The government of Saudi Arabia, for example, made the ability to filter a pre-requisite of public internet access, delaying any such access for a period of several years until the resources to filter were fully in place.

Citizens with technical knowledge can generally circumvent filters that a state has put in place. Some states acknowledge as much: the overseer of Saudi Arabia's filtering program, via the state-run Internet Services Unit, admits that technically savvy users can simply not be stopped from accessing blocked content. Expatriates in China, as well as those citizens who resist the state's control, frequently find up-to-date proxy servers through which to connect to the Internet, through which they can evade filters in the process. While no state will ultimately win a game of cat-and-mouse with those citizens who are resourceful and dedicated enough to employ circumvention measures, many users will never do so – rendering filtering regimes at least partially effective despite the obvious workarounds.

Pause here. Some of the earliest theorizing about control in the online environment suggested that such state-run control of Internet activity would not work. It's important to note that states such as China have proven that an ambitious state can, by devoting substantial technical, financial, and human resources, exert a large measure of control over what their citizens do online. States, if they want, can erect certain forms of gates at their borders, even in cyberspace and can render them effective through a wide variety of modes of control.

That does not mean that the issue is simple. For starters, states ordinarily need a great deal of help in carrying out filtering and surveillance regimes. Enter Internet Service Providers, many of whom require a license from the government in order to provide Internet access to citizens lawfully. Most filtering is effected by these private ISPs under

respective states' jurisdictions, though some governments partially centralize the filtering operation at private Internet Exchange Points – topological crossroads for network traffic – or through explicit state-run clearing points established to serve as gatekeepers for Internet traffic. Some governments implement filtering at public Internet access points such as the computers found within cybercafés. Such filtering can take the form of software used in many American libraries and schools for filtering purposes, or "normative" filtering – government-encouraged interventions by shop owners and others as citizens surf the Internet in a public place.

Sometimes the technical control is not enough. The exercise of more traditional state powers can have a meaningful impact on Internet usage that does not require the complete technical inaccessibility of particular categories of content. China, Vietnam, and Iran have each jailed "cyber-dissidents."[7] Against this backdrop, the blocking of Web pages may be intended to deliver a message to users that the government monitors internet usage. This message is reinforced by methods allowing information to be gathered about what sites a particular user has visited after the fact, such as the requirement of passports to set up accounts with ISPs and tighter controls of users at cybercafés.

As we learn more and more about how Internet filtering takes place, the problems of "governing" the Internet come more sharply into relief – about how control is exerted, about how citizens in one state can or cannot connect to others in another state, about the relationship between each state and its citizens, and about the relationships between states.

[7] Iran: Reporters Sans Frontières, "Appeal court confirms prison for cyber-dissident while blogger is re-imprisoned," available at http://www.rsf.org/article.php3?id_article=12564 (Feb. 15, 2005) ("Javad Tavaf, a student leader and the editor of the popular news website Rangin Kaman, which for a year had been criticising the Guide of the Islamic Revolution, was arrested at his home on 16 January 2003 by people who said they were from the military judiciary, which later denied it had arrested him."). China: Reporters Sans Frontières, Internet - China, available at http://www.rsf.org/article.php3?id_article=10749. Vietnam: Reporters Sans Frontières, Internet - Vietnam, available http://www.rsf.org/article.php3?id_article=10778.

2.2 Types of Content Filtered.

Around the world, states are blocking access to information online based upon its content for political, religious, and social reasons. Sensitivities within these categories vary greatly from country to country. Not surprisingly, these sensitivities track, to large extent, local conflicts. The Internet content blocked for social reasons – commonly pornography, information about gay and lesbian issues, and sex education information – is more likely to be the same across countries than the political and religious information to which access is blocked.

Several states carry out "heavy" filtering on certain topics, where our testing has shown that 50% or more of the sites we tested on a given topic – say, sex education – are inaccessible. Very rarely does any state manage to achieve complete filtering on any topic. The only areas in which 100% filtering is approached are pornography and anonymizers (sites that if themselves unfiltered would defeat filtering of other sites by allowing a user to access any Internet destination through the anonymizers' gateways). States like Burma, which reportedly listen in to email traffic, also block a high percentage of free e-mail service providers. Such complete, or near complete, filtering is additionally only found in countries that have outsourced the task of identifying pornographic sites to one of several for-profit American companies, and is inevitably accompanied by over-blocking. Outside of these three areas, we are consistently able to access some material of a similar nature to the sites that were being blocked.

2.3 Filtering and Over-breadth.

Wholly apart from the propriety of extensive government censorship as a threshold matter, Internet filtering is almost impossible to accomplish with any degree of precision. There is no way to stem the global flow of information in a consistently accurate fashion. A country that is deciding to filter the Internet must make an "over-broad" or "under-broad" decision at the outset. The filtering regime will either block access to too much or too little Internet content. Very often, this decision is tied to whether to use a home-

grown system or whether to adopt a commercial software product, such as SmartFilter, WebSense, or an offering from security provider Fortinet, each of which are products made in the United States and are believed to be licensed to countries that filter the Internet. Bahrain, for instance, has opted for an "under-broad" solution for pornography; its ISPs appear to block access to a small and essentially fixed number of "black-listed" sites. Bahrain may seek to indicate disapproval of access to pornographic material online, while actually blocking only token access to such material. The United Arab Emirates, by contrast, seems to have made the opposite decision by attempting to block much more extensively in similar categories, thereby sweeping into its filtering basket a number of sites that appear to have innocuous content by any metric.

Most of the time, states make blocking determinations to cover a range of Web content, commonly grouped around a second-level domain name or the IP address of a Web service (such as http://www.blogspot.com or 66.102.15.100), rather than based on the precise URL of a given Web page (such as http://www.blogspot.com/specificblog), or a subset of content found on that page (such as a particular image or string of text). Iran, for instance, has used such an approach to block a cluster of weblogs that the state prefers not to have reach its citizens. This approach means that the filtering process will often not distinguish between permissible and impermissible content so long as any impermissible content is deemed "nearby" from a network standpoint.

Because of this wholesale acceptance or rejection of a particular speaker or site, it becomes difficult to know exactly what speech was deemed unacceptable for citizens to access. Bahrain, a country in which we only found a handful of blocked sites, has blocked access to a discussion board at http://www.bahrainonline.org. The message board likely contains a combination of messages that would be tolerated independently as well as some that would appear to meet the state's criteria for filtering. Likewise, we found minimal blocking for internal political purposes in the UAE, but the state did block a site that essentially acted as a catalog of criticism of the state. Our tests can not determine whether it was the material covering human rights abuses or discussion of historical border disputes with Iran, but in as much as the discussion of these topics is

taking place within a broad dissention-based site, the calculation we project onto the censor in UAE looks significantly different than that for a site with a different ratio of "offensive" to approved content.

For those states using commercial filtering software and update services to try to maintain a current list of blocked sites matching particular criteria, we have noted multiple instances where such software has mistaken sites containing gay and lesbian content for pornography. For instance, the site for the Log Cabin Republicans of Texas was blocked by the U.S.-based SmartFilter as pornography, apparently the basis for its blocking by the United Arab Emirates. (Our research found that gay and lesbian content is itself often targeted for filtering, and even when it is not explicitly targeted, states may not be overly concerned with its unavailability.)[8]

As content changes increasingly quickly on the Web and generalizations become more difficult to make by URL or domain – thanks in part to the rise of simpler, faster, and aggregated publishing tools, like those found on weblog sites – accurate filtering is likely to get trickier for filtering regimes to address over time unless they want to take the step of banning nearly everything.

For example, free web hosting domains tend to group an enormous array of changing content and thus provoke very different responses from state governments. In 2004, Saudi Arabia blocked every page we tested on http://freespace.virgin.net and www.erols.com.[9] However, our research indicated the www.erols.com sites had been only minimally blocked in 2002, and the http://freespace.virgin.net sites had been blocked in 2002, but accessible in 2003 before being re-blocked in 2004. In all three tests, Saudi Arabia practiced by-URL blocking on www.geocities.com (possibly through SmartFilter categorization), only blocking 3% of over a thousand sites tested in 2004. Vietnam blocked all sites we tested on the www.geocities.com and members.tripod.org domains.

---

[9] Saudi Arabia blocked every page on www.erols.com except for the root page at www.erols.com itself, potentially indicating a desire to manage perceptions as to the extent of the blocking.

China's response to the same problem provides an instructive contrast. When China became worried about bloggers, they shut down the main blogging domains for a period of weeks in the summer of 2004. When the domains came back on-line, the blogging systems contained filters that would reject posts containing particular keywords.[10] Even Microsoft's MSN Spaces blogs software blocked writers from publishing terms like "democracy" from China. In effect, China moved to a content-based filtering system, but determined that the best place for such content evaluation was not the point of Web page access but the point of publication, and possessed the authority to force these filters on the downstream application provider. This approach is similar to that taken with Google to respond to the accessibility of disfavored content via Google's caching function. Google was blocked in China until a mechanism was put in place to prevent cache access.[11] These examples make clear the length to which regimes can go to preserve "good" access instead of simply blocking an entire service.

Alternate approaches that demand a finer-grained means of filtering, such as the use of automated keywords to identify and expunge sensitive information on the fly, or greater manual involvement in choosing individual Web pages to be filtered, are possible so long as a state is willing to invest in them. China in particular appears to be prepared to make such investment, one mirrored by choices demonstrated about more traditional media. For example, China allows CNN to be broadcast within the country with a form of time delay, so the feed can be temporarily turned off when, in one case, stories about the death of Zhao Ziyang were broadcast.[12] The global flow of information is tempered by the ingenuity of the censors, expressed through technical controls at many layers.

[10] http://www.opennetinitiative.net/bulletins/008/
[11] This mechanism turned out to be extremely rudimentary, as outlined a previous ONI bulletin (http://www.opennetinitiative.net/bulletins/006/).
[12] *See* http://cyber.law.harvard.edu/blogs/gems/tka/EPriestReactionPaper2.pdf

2.4 Law and Soft Controls.

Just as dozens of states use technical means to block citizens from accessing content on the Internet, most also employ legal and other "soft" means of control. Most states that filter use a combination of media, telecommunications, national security, and Internet-specific laws and regulatory schemes to restrict the publication of and access to information on the Internet. Most such states require Internet Service Providers to obtain licenses before providing Internet access to citizens. Some states – China, for instance, which has enacted special regulations to this effect – apply pressure on cybercafés and Internet Service Providers to monitor Internet usage by their customers. With the exception of Saudi Arabia, no country seems explicitly to communicate to the public about its process for blocking and unblocking content on the Internet. Most countries, instead, have a series of broad laws that cover content issues online, both empowering states that need it to carry out filtering regimes and putting citizens on general notice not to publish or to access content online that violates certain norms.

Often these soft controls are exercised through social norms or through control at the far edges of the network. Sometimes the state requires non-governmental organizations and religious leaders to register before using the Internet to communicate about the topics they work on. In China and in parts of Central Asian, very often the most fearsome enforcer of the state's will is the old woman on your block, who may or may not be on the state's payroll. The control might be exercised, as in Singapore, largely through family dynamics. The call by a local police force to the Malaysian blogger to come and talk about his publishing to the web might have as much of an effect on expression as any law on the books or technical blocking system.

Whether through advanced information technology, legal mechanisms, or soft controls, a growing number of states around the world are seeking to control the global flow of information. Ordinarily, this control takes the form of blocking that state's citizens from accessing certain information online. In other instances, the blocking stops the state's citizens from publishing information online, in effect disallowing people outside the state

from hearing the voices of the state's citizens. Most filtering regime results in a chilling effect on the use of information technologies as a means of free expression, whether for political, religious, or cultural purposes.

3.0 Filtering and Transparency as the Focus of the Internet Governance Debate.

The Internet governance debate could profitably take up the issue of filtering on the net. The practice of filtering is now a widely-known fact, but the hard problems that stem from this practice are infrequently discussed as a matter of public policy. The blocking and surveillance of citizens' activity on the Internet – by virtue of the network's architecture, an issue of international dimensions – calls for discussion at a multi-lateral level. Rather than fret over the finer points of the domain name system, the Internet filtering problem offers much more to be gained – even through frank discussion, if not action – and provides an exercise worthy of an extraordinary gathering of world leaders who want to talk about the global "Information Society."

There is certainly an argument to be made that Internet filtering is a private matter between a state and its citizens as to what information citizens may access online.[13] States that censor the Internet assert the right to sovereignty. From the state's perspective, the public interest, as defined in one state, say Saudi Arabia, is different from the public interest as defined by the state in Uzbekistan, or in China, or in the United Kingdom. States can, and do, exercise their sovereignty through control of the information environment.

Even if true, that argument should not end the conversation about Internet filtering. On broader level, the issue raised here is about interconnection between states and the

[13] Some states make an effort to suggest that their citizens (in Saudi Arabia and the UAE specifically) are largely in support of the filtering regime, particularly when it comes to blocking access to pornographic material. For instance, the agency responsible for both internet access and filtering in Saudi Arabia conducted a user study in 1999, and reported that 45% of respondents thought "too much" was blocked, 41% thought it "reasonable," and 14% found it "not enough." These studies stand for the proposition, in the context of our report, that some states that filter seek to make the case that their filtering regime enjoys popular support, not that such support necessarily exists.

citizens of those states – and ultimately about what sort of an Internet we want to be building and whether the global flow of information is a sustainable vision.

For instance, we have yet to join the ethical interests at play in filtering. States vary greatly in terms of how explicitly the filtering regime is discussed and the amount that citizens can come to know about it. No state that we studied makes its block list generally available.[14] The world leaders who gather periodically at the World Summit on Information Society and others at the center of the Internet governance debate could make the most of their leadership by taking up the mantle of seeking to establish a set of principles and best practices related to Internet filtering and the transparency related to filtering regimes.

This broader vision of Internet filtering – about what sort of a future we seek for the Internet – is just the sort of topic on which the Internet governance debate ought to focus. Even thought it is hard to talk about, the net is becoming each day larger and more fractured. Trends in favor of more speech from more people in more places around the globe – blogs, wikis, SMS, podcasting, and so forth – are countered by the increasing sophistication and reach of Internet filtering and surveillance practices. A richer understanding of the complexities at play in Internet filtering would help develop a foundation that does not yet exist for building a sustainable global network.

[14] Saudi Arabia publishes its rationale and its blocking practices on an easily accessible web site, at http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring.htm ("The Internet Services Unit oversees and implements the filtration of web pages in order to block those pages of an offensive or harmful nature to the society, and which violate the tenants of the Islamic religion or societal norms. This service is offered in fulfillment of the directions of the government of Saudi Arabia and under the direction of the Permanent Security Committee chaired by the Ministry of the Interior."). In Saudi Arabia, citizens may suggest sites for blocking or for unblocking, in either Arabic or English, via a public web site. Most sites include a block-page, indicating to those seeking to access a web site that they have reached a disallowed site. Most states have enacted laws that support the filtering regime and provide citizens with some context for why and how it is occurring, though rarely with any degree of precision. As among the states we have studied, China seems to obscure the nature and extent of its filtering regime to the greatest extent.