September 2004

A STARTING POINT:
LEGAL IMPLICATIONS OF INTERNET FILTERING

A Publication of the OpenNet Initiative

http://www.opennetinitiative.org

JEL Classifications: O380, K420, K390

A STARTING POINT:

LEGAL IMPLICATIONS OF INTERNET FILTERING

A Publication of the OpenNet Initiative[1]

ABSTRACT

In this paper, the Open Net Initiative (ONI) considers some of the legal implications of controlling access to Internet content through filtering. ONI -- a research partnership of the Berkman Center, University of Toronto's Citizen Lab, and the Cambridge Security Programme (University of Cambridge) -- documents Internet filtering by collecting empirical data about the parties who censor web traffic and the types of sites blocked in different countries. This paper considers the legal ramifications of this data.

Different governments offer a range of justifications for Internet filtering, including national security and the protection of community standards. While filtering regimes have a tremendous effect on issues such as civil liberties, international jurisdictional matters, and Internet governance, there are few established mechanisms for review and reform of Internet censorship. The paper highlights the importance of transparency, accountability, and inclusiveness in order to maintain a reliable, efficient, and global medium for communication.

Keywords: Internet, law, filtering, censorship

[1] The OpenNet Initiative is a collaborative partnership between three leading academic institutions: the Citizen Lab at the Munk Centre for International Studies, University of Toronto, Berkman Center for Internet & Society at Harvard Law School, and the Advanced Network Research Group at the Cambridge Security Programme at the University of Cambridge.

A STARTING POINT:

LEGAL IMPLICATIONS OF INTERNET FILTERING

A Publication of the OpenNet Initiative

Table of Contents

Introduction

Most countries censor Internet content in some fashion, typically by limiting the Web sites their citizens can view. We contend that the implications of Internet filtering are substantial and far-reaching, and ought to be understood well by those making policy related to information and communications technologies.[2]

The OpenNet Initiative seeks to answer basic factual questions of interest to a broad array of stakeholders: Who filters the Net? Precisely what content and types of Internet-based transactions are filtered? How is filtering implemented? How much do citizens know about filtering in their country? How much information on filtering could citizens realistically obtain?

This paper focuses on the legal and policy questions prompted by the OpenNet Initiative's study of Internet filtering. Under what authority, if any, does a given state filter? Are there any limits on a country's ability to censor Internet content? And what legal means can be employed to reform this practice?

1 Who Filters? Public v. Private.

The outcome of legal analysis often hinges upon who carries out the act in question. Often, an important distinction is whether the party responsible is a public or private actor.

1.1 Public Filters: Governments.

Internet filtering by governments is widespread. Almost every state – including countries with an ostensibly strong commitment to democratic principles and civil liberties – filters or censors access to Internet content in some way. However, the location, quantity, and manner of the filtering vary greatly. Filtering by state actors in the United States takes place primarily in schools and libraries, where the government can assert a "compelling interest."[3] China, Saudi Arabia, Iran, Singapore, Burma, and a series of countries in the CIS and Asia – where civil liberties are typically more restricted – filter more extensively. Such filtering may disallow access to certain Web sites, block or re-route e-mail traffic, or return search results different from those requested by the user.[4]

Among democratic states, Australia has received the greatest attention regarding its filtering practices. The Australian government passed legislation in 2000 requiring Australian ISPs to delete content deemed "disturbing or harmful" to people under 18 years of age from their servers. In addition, the government recommended that private companies add certain content to their filters, though Australian citizens are not required to use any blocking software.[5] The law necessarily applies only to content hosted within the country; this makes it a great deal more

---

[2] *See* Ronald J. Deibert & Nart Villeneuve, *Firewalls and Power: An Overview of Global State Censorship of the Internet*, in *Human Rights in the Digital Age* (Mathias Klang & Andrew Murray eds., forthcoming Oct. 2004). Deibert and Villeneuve discuss Internet filtering and its ramifications for government control and social policy.

[3] *See Reno v. Am. Library Ass'n*, 521 U.S. 844 (1997).

[4] The OpenNet Initiative documents the means and nature of filtering at http://www.opennetinitiative.org. *See* Jonathan Zittrain & Benjamin Edelman, *Documentation of Internet Filtering Worldwide, at* http://cyber.law.harvard.edu/filtering/.

[5] *See generally* Electronic Frontiers Australia, *Internet Censorship in Australia, at* http://www.efa.org.au/Issues/Censor/cens1.html (last updated Dec. 20, 2002).

limited than the blocking scheme enacted in China, for instance. This limitation notwithstanding, the law represents a proactive attempt by a democratic country to limit its citizens' Internet access as well as the material available on the Internet to users across the globe.

1.2 Private Filters: Companies.

Private parties are often centrally involved in Internet filtering. In many states where the government orders filtering, a state-run Internet service provider carries out the directive. In other cases, a government implements its policies through agreements with private companies. These companies, which might not even be based in the country seeking to filter, comply with the government's wishes for a variety of reasons, such as the possibility of financial gain or the need to obtain a government license to sell Internet access services to that state's citizens.

Consider the case of the world's most popular search engine, Google, during 2001. Pursuant to requests from the French and German governments, the localized Google search engines in those states, at http://www.google.fr/ and http://www.google.de/ respectively, removed certain "pro-Nazi" or racist sites from search results. While the French and German governments did not explicitly block access to those websites, their removal from Google hides them from most users, thus manipulating Google into a quasi-filter for both governments.[6]

Some private companies produce software that bars a user from accessing certain Web sites. This filtering may occur through a completely private transaction: a private citizen purchases filtering software from a private company for home use, perhaps to shield young children from accessing certain material. In addition, a number of states that filter utilize these software programs, many of which are produced by companies in the United States. Our study considers primarily those filtering practices where a government is involved in some fashion, with less emphasis on purely private transactions. Governments, though, often employ commercial software to automate filtering – in effect, these states outsource many decisions on proscribing content to private companies. For example, the Kingdom of Saudi Arabia uses Secure Computing's SmartFilter software to block access to content, such as pornography, that it feels is inappropriate.[7]

[6] *See* Jonathan Zittrain & Benjamin Edelman, *Localized Google Search Result Exclusions, at* http://cyber.law.harvard.edu/filtering/google/.
[7] *See* Jonathan Zittrain & Ben Edelman, *Documentation of Internet Filtering in Saudi Arabia, at* http://cyber.law.harvard.edu/filtering/saudiarabia/.

2 Law, Regulation, and Policy of Current Filtering Regimes.

The two components of a typical country's filtering regime are a justification for blocking certain material, and a set of laws that enable filtering.

2.1 Justifications for Laws and Regulations That Enable Filtering.

Countries usually justify the laws that enable filtering by invoking one of two broad themes: upholding "community standards" and ensuring "national security."

2.1.1 Upholding Community Standards.

The first common justification centers on protecting the "morals" or "standards" of the community. The Internet offers a broad array of information that is readily and freely available, much of which can trigger moral outrage, and sometimes outright fear, in certain viewers. States frequently seek to protect community standards by removing or blocking access to content they consider detrimental to the culture of their citizens. In many instances, this concern is expressed most acutely with respect to children. For example, one of Singapore's "main concerns" with the Internet is the ease of access to pornography by minors.[8]

The effort to uphold morality sometimes leverages legal concepts of "indecency" and "obscenity," whose definitions vary widely from country to country. Laws that support filtering regimes reflect these disparate definitions. South Korea banned content dealing with euthanasia and hacking[9], and, in a move that attracted widespread media attention, ordered local ISPs to block access to video footage of the gruesome beheading of a Korean hostage in Iraq.[10] Legislation in India blocks sites that "appeal[] to the prurient interest,"[11] and Australian law prohibits sites that include "information about crime or drug use."[12]

State efforts to uphold community standards can move beyond blocking pornographic or violent content to control religious or political material. For example, Egypt bans Internet content on "taboo issues" such as criticism of its president,[13] and Uzbekistan prohibits accessing materials critical of the country's president or based on religious extremism.[14] States vary in their transparency and specificity in defining community standards, and on the level of citizen participation in these decisions.

2.1.2 Ensuring National Security.

The second primary rationale for Internet filtering is national security. A number of states used the September 11, 2001 terrorist attacks in the United States, and the risk that terrorists might use the Internet to communicate, to justify greater restrictions on Internet content

---

[8] *See* Media Development Authority, *Internet Industry Guidelines*, *at* http://www.mda.gov.sg/medium/internet/i_guidelines.html.
[9] *See* Reporters Without Borders, *South Korea*, *at* http://www.rsf.org/article.php3?id_article=10774.
[10] *See* Kim Tae-gyu, *Internet Providers Urged to Block Hostage Video*, The Korea Times, June 24, 2004.
[11] *See* Sudha Nagaraj, *Ministry Braces to Keep Kids, Porno Sites Apart*, The Economic Times, July 7, 2001.
[12] *See* Reporters Without Borders, *Australia*, *at* http://www.rsf.org/article.php3?id_article=10746.
[13] *See* Reporters Without Borders, *Egypt*, *at* http://www.rsf.org/article.php3?id_article=10732.
[14] *See* Igor Rotar, *Uzbekistan: New controls on access to religious websites*, F18News, *at* http://www.forum18.org/Archive.php?article_id=86 (last updated June 19, 2003).

that could be detrimental to national security. Recent legislation often permits governments much greater latitude in monitoring and censoring Internet content viewed by their citizens.[15]

Other countries – particularly less democratic ones – filter the Internet more extensively, stating that such censorship is necessary to preserve national security. In China, protecting national security includes banning speech that could threaten "national unity."[16] Burma, Egypt, and Malaysia forbid any content that criticizes the ruling party. Liberia has blocked Web sites that contain "anti-Liberian material," while Zimbabwe excludes foreign sites that publish anything "likely to cause alarm or despondency."[17]

2.2 Laws That Enable Filtering.

Countries vary in the laws, regulations, and policies they enact to implement filtering regimes. Some states employ regulation specific to the Internet. In China, for instance, much of the legal work is accomplished through legislation relating to Internet access and agreements between the government and individual ISPs. Only nine ISPs in China have licenses to provide Internet access, making it easier for the government to centralize control than in countries where larger numbers of ISPs can lawfully provide access. In the past, China has limited the search results available through Google and other search engines; at other times, the state has prohibited search engines from operating in their normal fashion.[18] Overall, more than sixty laws limit the content available to Chinese Web users.[19] Yet no standards are set forth in law as to what content is to be filtered, nor is there any official admission of filtering.

Other states, such as Burma, use laws designed to regulate the media in general to police the Internet's content. India is currently considering the Communications Convergence Bill, which would establish a set of broad-based laws governing the content and transmission of all communications in India, regardless of the medium.[20] Some countries control Internet access and content based on concerns about effects on more established media. For example, Canada limits the amount of video streaming available due to interference with established broadcasting regulations.[21] Other states limit the availability of Internet telephony through Voice Over Internet Protocol (VoIP) because of protests from telecommunications providers, which are often state-run monopolies.

Finally, countries use laws of general applicability to restrict Internet content. Foremost among these are intellectual property laws. A number of countries use existing copyright regimes to justify limitations on content ranging from entertainment to news. Other states use laws prohibiting defamation or libel to prevent access to certain Web sites. By claiming a particular site defames a government figure, such as a party leader, a state may justify removing

---

[15] The USA PATRIOT Act passed by the United States Congress on October 26, 2001, for example, makes it easier for US government officials to monitor a user's Internet traffic. *See Bill Summary & Status, USA PATRIOT Act*, *at* http://thomas.loc.gov/cgi-bin/bdquery/z?d107:h.r.03162:.

[16] *See* Reporters Without Borders, *China*, *at* http://www.rsf.org/article.php3?id_article=7237.

[17] *See* Privacy International and the GreenNet Educational Trust, *Silenced: An International Report on Censorship and Control of the Internet* 20, *available at* http://www.privacyinternational.org/survey/censorship/Silenced.pdf.

[18] *See* Jonathan Zittrain & Benjamin Edelman, *Empirical Analysis of Internet Filtering in China*, *at* http://cyber.law.harvard.edu/filtering/china/.

[19] *Silenced* at 54.

[20] *See* Rahul Ghosh, *Media Convergence*, The Statesman, November 29, 2001.

[21] *Silenced* at 21.

access to it. Governments may use laws forbidding dissension or otherwise acting against the government to create *de facto* Internet censorship even in the absence of Internet-specific rules.

3 Legal Problems of Internet Filtering.

3.1 Civil Liberties: Speech, Press, Privacy, Religion, and Association.

Internet filtering often risks violating citizens' state-recognized civil liberties. In many countries, citizens can rely upon one or more of the following rights: freedom of expression (whether individually or as a member of the press), privacy, religion, and association. The nature and extent of these civil liberties vary substantially. The United States, for instance, has a tradition of strong, though frequently threatened, civil liberties; in some countries, citizens have no liberty protections at all. Civil liberties' protections often vary based on the actor accused of infringement – for example, most U.S. safeguards apply only against state actors. As a result, the legality of different types of filtering will depend in part upon the parties involved. The legal challenges to the Communications Decency Act and its progeny in the United States highlight the core of these problems from a civil liberties perspective.[22]

A vital issue raised by every filtering regime is the extent to which blocking is both over-broad and under-inclusive – cardinal sins to those who advocate free speech and those concerned about Internet content respectively. Thus, filtering may infringe on civil liberties unnecessarily. The United States Supreme Court, for instance, upheld a requirement for Internet filtering of material "harmful for minors" in public libraries as a condition of receiving federal financial support.[23] However, commercial software filters often block material unrelated to this goal, while missing vast amounts of material that violates the standards the U.S. seeks to uphold.[24] The Internet is far too vast and dynamic for current filtering technologies to be particularly good at what they are meant to accomplish. The technology has not yet caught up to the aspirations of the law.

3.2 Jurisdiction.

Legally, jurisdiction refers to the power and willingness of a sovereign to regulate and control a particular area or problem. Traditionally, states claim sovereignty, and hence jurisdiction, over the physical territory they control and the people who inhabit it. States create and enforce laws to assert control within their jurisdiction. Activities that cross political boundaries, though, challenge this concept of jurisdiction. For example, if a United States citizen acts in Japan in a way that harms people in Brazil, which country has jurisdiction? The Internet exemplifies this problem, as filtering demonstrates.

When a state filters packets flowing through a network within its geographic boundaries, that state regulates and affects the communications of citizens not only in its own territory, but potentially worldwide. The filtered communications might include e-mail between a citizen of

[22] *See* Electronic Privacy Information Center, *Communications Decency Act*, *at* http://www.epic.org/free_speech/CDA/ (last updated Feb. 2, 2002).
[23] *See United States v. Am. Library Ass'n*, 539 U.S. 194 (2003).
[24] *See* Benjamin Edelman, *Sites Blocked by Internet Filtering Programs*, *at* http://cyber.law.harvard.edu/people/edelman/mul-v-us/.

the filtering country and one of a non-filtering country; one state's control over e-mail affects the ability of both states' citizens to exchange information. Filtering might simply block access within a country's borders to certain Web sites, or it might alter network traffic within its borders and prevent access even by non-citizens. Internet control is geographically dispersed, falling under multiple jurisdictions. Conflicts inevitably arise when a party in one country uses the Internet in a way that harms a party in another country. The jurisdictional issues inherent in these conflicts fit into three primary categories: personal and subject matter jurisdiction, choice of law, and enforcement.[25]

3.2.1 Personal and Subject Matter Jurisdiction.

Sovereigns traditionally divide jurisdictional analysis along two axes: control over the defendant in a legal dispute (personal jurisdiction) and control over the type of dispute (subject matter jurisdiction). Personal jurisdiction involves issues of fairness – whether a person should be subject to a state's regulation – and authority – whether a state can effectively enforce its mandates. Subject matter jurisdiction involves questions of institutional competence; for example, whether a particular court is authorized or has the expertise necessary to adjudicate a given dispute. Internet regulation raises issues at the heart of personal jurisdiction in particular.

For example, an Australian businessman, Joseph Gutnick, sued the U.S. publishing company Dow Jones in Australia.[26] Gutnick claimed that Dow Jones defamed him by publishing an article critical of him in its on-line issue of *Barron's*. The High Court of Australia asserted jurisdiction based on sales of on-line subscriptions to *Barron's* to Australians by Dow Jones and based on Gutnick's Australian citizenship. Similarly, the Superior Court of Paris held that it was competent to hear a case against the U.S.-based Internet company Yahoo! because Yahoo! allowed French citizens to participate in auctions of Nazi paraphernalia in violation of French law.[27] The French court ordered Yahoo! to take all technically possible measures to prevent access by French citizens to sites with forbidden Nazi content and fined the company 10,000 francs. In contrast, a recent decision by a United States federal appellate court found that U.S. courts lacked personal jurisdiction over the two French organizations who brought the *Yahoo!* case because those organizations had insufficient contacts with the U.S. to justify exercising authority over them.[28]

Jurisdiction limits a plaintiff's available remedies. A party injured by a foreign government's Internet filtration typically has limited legal recourse. She must choose between pursuing action in that state's courts, which will likely be unsuccessful either because filtering is legally authorized there or because government actions are protected by the doctrine of sovereign immunity[29], or bringing suit in her home jurisdiction, which may lack authority to hear the

---

[25] *See* Jonathan Zittrain, *Be Careful What You Ask For: Reconciling a Global Internet and Local Law, available at* http://cyber.law.harvard.edu/home/uploads/204/2003-03.pdf.

[26] *See Dow Jones & Company, Inc. v. Gutnick* (2002) 194 A.L.R. 433.

[27] *See La Ligue Contre le Racisme et l'Antisemitisme v. Yahoo!, Inc.*, T.G.I. de Paris (May 22, 2000) (*see* English translation *at* http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm).

[28] *Yahoo! Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme & L'Union Des Etudiants Juifs de France*, No. 01-17424 (9th Cir. 2004), *available at* http://www.ca9.uscourts.gov/ca9/newopinions.nsf/D079531C495BC5E288256EF90055E54C/$file/0117424.pdf?openelement.

[29] The doctrine of sovereign immunity typically protects governments and their officials from lawsuits unless the government specifically authorizes the suit or, more commonly, waives its protection through statutes.

dispute or the power to enforce a judgment. In some cases, though, a party may be able to pursue actors indirectly responsible for the filtering, such as developers of Internet filtering software located in her jurisdiction.

Jurisdictional conflicts between states over Internet issues can lead to legal and even trade disputes. For example, a federal district court in California ruled that the French judgment against Yahoo! could not be enforced in the United States, despite its validity in France, because of the protections for speech in the U.S. Constitution.[30] The Ninth Circuit Court of Appeals overturned the decision, finding that the U.S. courts had no personal jurisdiction over the French organizations in the Yahoo! case because they had not yet tried to enforce the French judgment against Yahoo!'s assets in America.[31] Should the victorious French plaintiffs move to collect from Yahoo!'s U.S. resources based on the French judgment, though, the conflict between American and French legal standards for Internet speech will recur. Similarly, the state of Antigua and Barbuda brought a case against the United States before the World Trade Organization over Internet gambling, which is banned by the U.S. but constitutes a major industry for the island state. The WTO ruled that the U.S. ban violates international trade requirements.[32] The Internet's global content distribution and the role of multinational media companies make clashes between states regarding jurisdiction inevitable. Disputes may be resolved by international coordinating bodies such as the WTO or agreements between countries[33], or may lead to inconsistent results in different jurisdictions.

3.2.2 Choice of Law.

Choice of law (also known as private international law) issues involve deciding which jurisdiction's laws should control a dispute or conflict. This analysis is independent of personal and subject matter jurisdiction questions, since a state can decide to hear a case but apply the laws of another state. In cases where more than one jurisdiction's laws could apply, courts typically try to determine which jurisdiction has the most significant relationship to the transaction or case at issue. This approach is difficult for Internet-based disputes, since the jurisdictions of the content provider, Internet Service Provider, and user may have equally strong claims to control. States may try to resolve these problems ahead of time through multilateral coordinating agreements. For example, the European Union's Brussels I Regulation governs these decisions for most EU countries.

In practice, however, states prefer to apply their own laws to disputes. This is particularly likely with filtering disputes, because filtering involves two issues at the core of a state's sovereignty: the government's authority to regulate its telecommunications infrastructure, and local cultural standards regarding unacceptable content. States are likely to view these interests as determinative in choice of law decisions. Thus, while filtering presents important

---

[30] *See Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 169 F. Supp. 2d 1181, 1192-94 (N.D. Cal. 2001).

[31] *Yahoo! Inc.*, No. 01-17424 (9th Cir. 2004).

[32] *See* Matt Richtel, *Trade Group Says U.S. Ban on Net Gambling Violates Global Law*, N.Y. Times, Mar. 26, 2004, at C5; *see also Gambling Ban Struck Down*, Washington Post, Mar. 25, 2004, at E2 (noting that "Antigua-based Internet companies handle one-fourth of online bets in a global industry worth $6.1 billion, and about one-sixth of Antigua's $200 million annual revenue is derived from it").

[33] Antigua and the U.S. are attempting to negotiate a resolution to the Internet gambling dispute. *See Antigua and US attempt to settle gambling dispute*, Caribbean Net News, July 2, 2004, *at* http://www.caribbeannetnews.com/2004/07/02/dispute.htm.

choice of law or private international law issues, resolution of these questions is weighted towards a state asserting the primacy of its laws in a dispute.

3.2.3 Enforcement.

The ability to enforce a judgment imposes a practical limit on a sovereign's jurisdiction. While an unenforceable judgment may still have value – for example, to signal a state's position on a contested issue or to affirm a litigant's abstract rights[34] – it does not generally alter a defendant's behavior or compel obedience. Thus, the decision of the U.S. federal district court in the *Yahoo!* case paid deference to France's authority to prescribe objectionable content within its territory, but refused to allow France to enforce that regulation through any judgment against Yahoo!'s American assets.[35] Traditionally, enforcement required a state to have either direct control over the defendant or her property, or a binding agreement with another state requiring enforcement of the first state's judgments. For example, the Hague Convention on Private International Law has created a Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters to address enforcement.[36] The convention would have an effect on adopting states similar to that of the U.S Constitution's Full Faith and Credit clause[37], which requires American states to recognize final, binding judgments issued by sister states. Absent one of these two arrangements, states were generally powerless to enforce decisions beyond their borders.

Filtering, however, makes enforcement easier for sovereigns. A state's control over Internet infrastructure, service providers, content providers, or users can be sufficient to enforce its determinations through filtering.[38] Generally, a state's enforcement power is limited when a defendant has no property or physical presence within that state's geographical boundaries. With filtering, though, the state can enforce its dictates by limiting or preventing access to its communications infrastructure. Enforcement is accomplished through prevention, not punishment.

One potential locus for enforcement, particularly in developing countries, is an Internet exchange point (IXP). Internet exchange points allow users within a country to exchange and access Internet data without routing it outside the state's borders, increasing efficiency and reducing expense. In countries with multiple ISPs, setting up an IXP can reduce costs for providers and subscribers. For example, countries that use satellite dishes for Internet

---

[34] *See Citron v. Zündel*, [2002] T.D. 1/02 2002/01/18 (Can. Human Rts. Trib.). In *Zündel*, the Canadian Human Rights Tribunal found it had jurisdiction to decide a case by a Canadian Holocaust survivor against a U.S. citizen who supplied content to an anti-Semitic Web site run by a U.S. Internet Service Provider. The Tribunal concluded that posting to the site violated Canadian human rights laws. The Tribunal was "extremely conscious of the limits of the remedial power available in this case" but stated that a "remedy awarded by this, or any Tribunal, will inevitably serve a number of purposes: prevention and elimination of discriminatory practises is only one of the outcomes flowing from an Order issued as a consequence of these proceedings". *Zündel* at 298, 300.

[35] *See Yahoo!*, 169 F. Supp. 2d at 1192-93.

[36] *Available at* http://www.hcch.net/e/conventions/draft36e.html (adopted Oct. 30, 1999).

[37] U.S. Const. Art. IV, § 1.

[38] *See* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 Ind. J. Global Legal Stud. 475, 481 (1998). Goldsmith notes that a state "retains the ability to regulate the extraterritorial sources of local harms through regulation of persons and property within its territory" and that this is "how nations have begun to regulate local harms caused on the Internet by extraterritorial content providers". *Id.* Sovereigns can "'regulate in-state entities that supply or transmit information" and "regulate in-state hardware and software through which Internet transmissions are received" to control content. *Id.* at 481-82.

connectivity may route traffic via satellite to a network service provider based in the United States or Europe. Thus, an e-mail message from a subscriber to ISP A in the country to a user of ISP B routes from A's servers through the U.S. to B's servers. This is less efficient and more costly than routing the packets locally, within the country. To avoid this inefficiency, ISPs coordinate the creation of exchange points to allow them to exchange data between their networks within the country's borders. Thus, data exchanged between users in that country routes through the IXP, while data to or from foreign sources passes through other network channels. Establishing an IXP requires overcoming two challenges, one technical and one financial. The technical obstacle is that each ISP must create a high-bandwidth connection to the central location where the IXP will be located. ISPs must agree on the location before this can occur. The financial challenge is that ISPs must negotiate and sign peering agreements with each other regarding exchanging and carrying traffic – in addition to obtaining any required governmental approval. Peering arrangements can be free (each ISP carries the other's traffic, in return for the same benefit), for a flat fee, or for a fee based on traffic. In theory, a government might monitor or block Internet content at an IXP. However, this is not likely, for three reasons. First, most Internet traffic travels across national borders, not within a country, so filtering at an IXP affects only a minority of content. Second, filtering at an IXP is relatively expensive since the exchange point aggregates traffic; a filtering government would need computing resources that were larger and more capable than those used on a per-ISP basis. Third, IXP filtering may be vulnerable to circumvention; for example, dissidents exchanging e-mail within a country could avoid an IXP by routing mail through foreign sites such as Hotmail or Yahoo! mail. While IXPs could theoretically be targeted for filtering by governments, the cost challenges of doing so and the limited traffic flowing through the exchange points mitigate against this possibility, and it is unsurprising that there are no reports of states using IXPs for this purpose.

Thus, Internet filtering effectively increases a sovereign's jurisdiction. Traditionally, a state's ability to decide a case was limited geographically by its power to enforce its judgment. With Internet filtering, though, a state can control a defendant's conduct by preventing that party's content from reaching its citizens. This expansion comports with the concept that a state has power to prevent harms to and assert control over its citizens, but it also expands greatly the number of sovereigns with actual or potential power over Internet content.

3.3 Internet Governance.

The quandary of Internet governance is a close cousin to the jurisdiction question. Filtering sharpens the problem of governance by effectively devolving control from international organizations and standards-setting bodies to individual states and ISPs.[39] The December 2003 World Summit on the Information Society (WSIS) and its aftermath put the Internet governance issue back on central stage.[40] The focus is shifting from the original disputes over domain name allocation and the structure of the Internet Corporation for Assigned Names and Numbers (ICANN) to broader issues like filtering, spam, network security, and other tricky, distributed problems.

There is no consensus as to how this debate will play out. Between late 2003 and the next WSIS meeting in Tunis in 2005, many people are focusing on the Internet governance

[39] *See* Jonathan Zittrain, *Can the Internet survive filtering?*, CNET News.com, July 23, 2002, *at* http://news.com.com/2010-1071-945690.html.
[40] *See World Summit on the Information Society at* http://www.itu.int/wsis/.

question, as it was the primary "call to action" of the Geneva WSIS meeting. As Internet governance can have sweeping ramifications for Internet filtering – perhaps even enforcing a certain level of censorship across the World Wide Web – an understanding of filtering practices, grounded in reliable empirical research, is an important input to this debate.

3.4 International Law.

International law provides few obvious tools to analyze Internet filtering, though the potential surely exists.[41] Countries often make law through multilateral agreements that bear on Internet law and regulation. For instance, trade agreements frequently include provisions related to intellectual property that could affect filtering issues. Requirements of free trade between states might also, on their face, be violated by filtering practices that impede commercial transactions between individuals or companies in the relevant countries. International human rights law might also apply when states block certain sensitive content (for example, Web-based information on broad public health issues such as SARS). In at least one case, a movement began to categorize one company as a human rights violator due to its complicity with a state's systematic control over the Internet use of its citizens.[42] A next generation of international humanitarian law, some have argued, might also include protections for access to communications.

3.5 Telecommunications Law.

Like international law, the global and national telecommunications regulatory regimes might prove relevant to Internet filtering. The Internet and telephony systems have traditionally been treated separately. Telecommunications have been extensively regulated, while Internet communications have been regulated to a lesser extent. As more voice and other previously telephony-based communications travel over the Internet through technologies such as VoIP, policy makers increasingly consider treating the networks as converged. The practice of Internet filtering, though unlikely to violate existing telecommunications laws, is plainly relevant to the development of telecommunications law and policy.

3.6 Other Kinds of "Law."

The most important code in Internet filtering is not legal code, but computer code.[43] Internet filtering is often set in motion by legislation, regulation, or policy, but then rendered effective and enforced through software. Software code avoids the jurisdictional pitfalls of its legal counterpart; enforcement is automatic and, in theory, absolute. Countries often contract with companies in other states for this code. Legislation can re-enter the picture to prohibit circumvention of filtering regimes. The interplay between these two forms of code, as well as social norms and the actions of commercial entities, is essential to the story of global Internet filtering.[44]

---

[41] *See* United Nations, *International Law*, *at* http://www.un.org/law/.

[42] *See* Human Rights Watch, *Yahoo! Risks Abusing Rights in China*, *at* http://www.hrw.org/press/2002/08/yahoo080902.htm (last updated Aug. 9, 2002).

[43] Lawrence Lessig outlined and popularized a series of insights about the interplay of "East Coast Code" (legislation) and "West Coast Code" (software programming) in *Code and Other Laws of Cyberspace* (1999).

[44] *See id.* Lessig also builds out a typology of four key regulatory factors in the Internet setting: law, code, markets, and norms.

4 Are There Any Effective Legal Limitations On A State's Ability to Filter?

Each state maintains independent control over the nature and extent of Internet access of its citizens. While some states, such as Cuba, severely limit Internet and e-mail access, others allow access to the Internet but heavily censor the content available. There are no meaningful external legal checks on a country's ability to filter the Internet access of its citizens, as there are no international treaties or declarations safeguarding a free and open Internet. Currently, the United Nations takes no stance on the Internet, though proposals have been put forth to bring Internet governance under its jurisdiction.[45]

Market forces may help ensure a minimum level of Internet access. Internet access results in well-substantiated productivity gains for an economy. Once a country allows its citizens to access the Internet, it likely cannot eliminate this privilege without considerable outrage and potential dissension. For instance, while China heavily filters its citizens' Internet content, it does not eliminate access completely. Chinese citizens would not likely tolerate an outright prohibition, even in an autocratic state able to enforce such a rule. When China blocked access to Google in September 2002, redirecting users to government-controlled search engines, popular opposition forced the government to rescind the ban and to target individual sites listed by Google instead.[46] However, this market check does not solve the filtering problem for at least two reasons. First, filtering often takes place without detection. While a complete lack of Internet access is obvious, only users who know of the existence of blocked Web sites will know that their access has been limited. This lack of knowledge contributes to the problem of complacency. Second, since all states filter to some extent, citizens may come to accept a certain degree of filtering.

It is unlikely that even the most effective efforts of the technical community could stop filtering from occurring in most countries. The Internet is a network of networks. If one network behaves erratically, there is little that operators of the broader network can do to bring that erratic network back into line. China, for one, strives to create a "China Wide Web" with its own distinct set of rules. The engineers who set standards for the World Wide Web are unlikely to affect filtering on the China Wide Web or even the filtered Internet of less populous, less powerful states.

5 Toward a Reform of Global Internet Filtering.

Those who believe current regimes of Internet filtration pose a problem and want to do something about it face a daunting challenge. There is no obvious fix, nor even a universally accepted notion of what the problem encompasses. Reform might involve a combination of legal

---

[45] *See* WSIS General Secretariat, *Report of the Geneva Phase of the World Summit on the Information Society, at* http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0009!R1!PDF-E.pdf (asking the "Secretary-General of the United Nations to set up a working group on Internet governance").

[46] *See* Joseph Kahn, *China Seems To Refine Bid To Restrict Web Access*, N.Y. Times, Sept. 14, 2002, at A5 (noting the "overwhelmingly negative reaction to blanket blockage" since "Google is widely used to get access to an array of documents and Web addresses that use Chinese characters"); *see also* The OpenNet Initiative, *Google Search & Cache Filtering Behind China's Great Firewall*, *at* http://www.opennetinitiative.net/bulletins/006/ (last updated Sept. 3, 2004) (describing techniques China uses to block searches for sensitive keywords).

or diplomatic elements. More likely, though, positive change will require a combination of illuminating and expanding upon the problem, putting Internet technologies to work, and applying pressure through social norms.

Diplomatic pressure by a powerful state or coalition might suffice to convince a country to change its policies on cyberspace freedom. Similar kinds of pressure helped to ensure greater human rights in China and the dissolution of apartheid in South Africa – arguably more compelling causes, but ones demonstrating a plausible path to change. In addition to moral pressure, states can apply economic pressure through sanctions and trade restrictions. In this manner, the international community can influence domestic Internet policy.

The United States may yet act in this area. A bill introduced in the U.S. Congress declares that all people worldwide have a right to unrestricted use of the Internet. The bill would also create an Office of Global Internet Freedom to police these rights.[47] This bill, however, raises a host of questions. Why should the U.S. set the standard by which filtering is judged? How could such a bill possibly be enforced? What would the authority of such an Office be?

Any type of legal or diplomatic solution risks interfering with a state's traditional sovereignty. There is wide disagreement as to what content should be accessible to citizens. The definition of "indecent" material in the United States would let pass material that would be deemed off-limits in much of Europe, and certainly in countries like Saudi Arabia or other parts of the Middle East. A quick survey of national views on "indecency" reveals the enormous complexity of formulating an international standard.[48] It seems unlikely that any single standard could serve as an international model. It seems equally unlikely that any central coordinating body could serve as decision-maker, as many believe that "an international body has no right to regulate the content of Web sites."[49]

Thus, people within a given country, or the international community at large, may well be able to affect a state's ability to censor Internet information. Illuminating the scope, contours, and consequences of Internet filtering is an essential first step toward change – and is one of the core charges of the OpenNet Initiative.

---

[47] *See* The House Policy Committee, *Tear Down This Firewall*, *at* http://policy.house.gov/html/news_item.cfm?id=112 (last updated Sept. 19, 2002).

[48] In Algeria, indecency is defined as "material that undermines public order and morale" and includes the "denigration of the president through insults or defamation." Kazakhstan has a similar prohibition against "harming the honour and dignity" of the President. Bahrain blocks sites that are "platforms for spreading biased news, rumours and lies." Burma regulates any online writings "detrimental to the interests of the Union of Myanmar and that are directly or indirectly detrimental to the current policies and secret security affairs of the government." For a more detailed list, *see Silenced* at 20–21.

[49] *See* Chris Hawley, *Countries, companies debate U.N. control over Internet*, The Detroit News, Mar. 29, 2004, *at* http://www.detnews.com/2004/technology/0403/31/technology-105722.htm.

6 Conclusion.

Internet filtering seeks to control what content users – in a country, in a company, or in a home – can access. The filtering entity must confront the clash of local standards and norms with an international medium whose design resists barriers and blocks. This paper assesses which actors try to limit access to Internet content, the material to which they object, and the means they employ. In the end, there is no simple way to establish and enforce a single legal standard for Internet content across every state. Countries with widely divergent perspectives on governance, civil liberties, and culture are unlikely to achieve consensus on a filtering regime. Differences among actors, standards, ideals, and implementation are inevitable.

However, reform of filtering attempts is both desirable and possible. First, changes to Internet filtering would be beneficial. ONI believes that any filtering regime should embrace three cardinal principles: transparency, accountability, and inclusiveness. Transparency requires defining clearly and narrowly the content that is blocked or prohibited; this informs content providers of what material is not permitted and helps citizens understand the values that filtering seeks to implement. Accountability creates a feedback system where filtering decisions can be challenged and where actors, such as government agencies, must justify and defend their actions or failures to act. Inclusiveness involves citizens in decisionmaking about filtering, appropriate material, and the balance of control between public and private actors. Unfortunately, most current filtering systems fail to incorporate one or more of these principles. China, for example, fails the first two requirements and permits only limited citizen interaction for the third (in the form of allowing users to suggest pornographic Web sites to block).[50]

Reform is also an attainable objective. International organizations, coalitions, and states may be unable to enforce their views, but even symbolic regulations and standards have power. Tools such as trade agreements and diplomatic pressure can convince states to alter their filtering behavior. Internally, citizens can appeal to traditional legal doctrines such as jurisdictional concerns and civil rights protections to guarantee certain levels of freedom for Internet access. Observers such as ONI can use strategic analysis, monitoring, and circumvention to expose filtering techniques and to alert people to the content they are denied, in the hope that knowledge will generate demands for transparency and reform.

In its future research, ONI intends to examine informal filtering practices, such as the adoption and enforcement of acceptable use policies by ISPs and self-censorship by entities such as search engines based on requests by governments and internal assessments of what content is acceptable. These informal methods also constitute a type of law that effectively control what users can access – and may prove less transparent and visible than formal legal content restrictions.

Filtering is inevitable; nearly all Internet users would agree to restrictions on material such as child pornography or instructions on creating weapons of mass destruction. However, public and private filtering today is far from optimal, and ONI believes that legal and technical explication of these systems will benefit policymakers worldwide. ONI will combine legal

[50] *See Ensuring clean online environment*, China Daily, *at* http://www.chinadaily.com.cn/english/doc/2004-07/31/content_353536.htm (last updated July 31, 2004) (noting that the "Ministry of Public Security set up a hotline and a website for people to report porn websites").

analysis, technical exploration, and country-specific testing to describe the state of Internet filtering worldwide and to urge necessary reform.