Before the

National Telecommunications and Information Administration,
U.S. Department of Commerce
Washington, DC 20230

In the Matter of	)	
	)	
Global Free Flow of	)	
Information on the Internet	)	Docket No. 100921457–0457–01

Comments of The New America Foundation, Free Press, Electronic Frontier Foundation, Public Knowledge, Reporter Without Borders, American Civil Liberties Union

December 6, 2010

1. Introduction

We commend the National Telecommunications and Information Administration (NTIA) inquiry into restrictions on the free flow of information on the Internet, particularly at a time when the U.S. government's approach to Internet policy has been marked by dissonance and contradiction. Between the State department's push for Internet freedom,[1] the Federal Communication Commissions' regulator efforts on Net Neutrality, the administration's push for more extensive Internet surveillance in the name of national security, and the strengthening of website takedown and censorship mechanisms in the name of copyright enforcement, the U.S. government's actions in aggregate send contradictory signals about Internet control versus Internet freedom.

We respectfully take this opportunity to provide a range of examples where policies create environments that restrict the free flow of information. Some examples demonstrate restrictions resulting from direct government action, such as Internet filtering regimes and censorship via intermediary platforms. However, we also take this opportunity to demonstrate how government

[1]Hillary Rodham Clinton, *Remarks on Internet Freedom*, January 21, 2010 http://www.state.gov/secretary/rm/2010/01/135519.htm

inaction can allow companies to stand in the way of freedom of speech and communication. We stress that this is not an exhaustive list of isolated incidents but part of a range of policies that can result in the restriction of the free flow of information on the Internet. While repressive regimes are in many cases intentionally restrictive, otherwise well-intentioned policies of democracies – in the pursuit of security, child protection, copyright protection, and other commercial aims – can also create barriers to the free flow of information, or provide justification for more oppressive censorship.

In our filing, we stress that the Internet is a shared resource, with over a billion networked devices and a global community created by over 26,000 independent and autonomous networks.[2] All Internet users benefit from spillover effects.[3] Similar to common pool resources like water and air that sustain and nourish life, the Internet provides value across borders by enabling and nourishing innovation, collaboration, and new forms of communication and cooperative development. The interconnection of ideas, economies, and innovation between people throughout the world maximizes the democratic and economic potential of the Internet. The effects of information policy are far reaching, impacting human rights and freedoms of expression, and restrictions can hide government abuses, prevent organizing, or create chilling effects.[4] Whether caused by insufficiently accountable or transparent state interference or weak regulation of private actors, restrictions on information flows can occur throughout the Internet ecosystem. As an added challenge, countries connected by the Internet have vastly differing cultural norms, levels of political accountability in their governance, and commercial and economic regulatory regimes, further complicating any potential harmony in international information policy frameworks.

In pursuing the free flow of information on the Internet, the NTIA must consider the global implications of long-term policies across varying legal regimes and political systems. In approaching this issue we urge the NTIA to act on principles of openness, contributing to a consistent U.S. government policy domestically and internationally to promote the exchange of free thought, democracy, innovation, and information.

---

[2] *Information and Communications Technologies OECD Communications Outlook 2009*

[3] *See* Brett Frischmann & Mark Lemley, "Spillovers", 107 Colum.L.Rev. 257 (2007).

[4] For example, following riots in the Xinjiang province in July 2009, the Chinese government cut off Internet access to the province for six months and Iran blocked Facebook and Twitter before the election in 2009. *See* Rebecca MacKinnon *Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom*, presented at Liberation Technology in Authoritarian Regimes, October 11-12, 2010. See also Ali Sheikholeslami, Iran Blocks Facebook, Twitter Sites Before Elections (Update1), Bloomberg, May 23, 2009, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=anh.uW3gNZp4.

2. Types of Restrictions to the Free Flow of Information on the Internet

Direct Government Censorship

The clearest examples of restrictions are cases in which government-mandated filters or policies actively block citizens' access to information. These examples include government-imposed network traffic filtering technology resulting in the blocking of access to specific websites, restricting the access of specific users or a class of users, or creating barriers to accessing the Internet.

Network level Filtering

Access to information can be restricted by placing filtering technology directly into the networks. Many countries employ filtering technology to block access to types of content, keywords or applications by preventing data transmissions. For example, the government of China has implemented a nationwide system of Internet filtering tamper with DNS resolution or block access to specific IP addresses. As described by the Open Net Initiative (ONI), China's filtering system also uses TCP reset for "content filtering by keyword targets...regardless of where [content] is hosted."[5] Filters check for keywords in both the header and content of packets of data, and terminate the connection if a prohibited keyword is detected.

China is not alone among countries that filter at the network level. For example, Iran and Pakistan both use network level filters. According to ONI, all public Internet traffic in Iran is routed through proxy servers where filtering software can block specific keywords or websites.[6] Pakistan has attempted to block "pornographic and blasphemous" websites through content filters placed at Internet exchanges.[7] Blogspot.com was blocked entirely during 2006 in addition to a number of human rights websites.[8] Facebook.com was blocked in Syria in November 2007, and Blogger, YouTube, and political websites have also reportedly been blocked.[9] The blacklist maintained by National Telecommunications Corporation in Sudan, filtering content before entering the country, includes websites viewed to be blasphemous to Islam.[10] In total, the Saudi authorities claim to have blocked some 400,000 websites, including the site *newarabia.org*, a political discussion forum, and the blog hosting website blogger.com In Tunisia, censored websites include those for political opposition, independent news, and human rights organizations.[11] Websites now inaccessible include those of *Tunisnews*, *Nawaat*, *Tunisonline*,

[5]OpenNet Initiative *Internet Filtering in: China*, 17.
[6]OpenNet Initiative *Internet Filtering in: Iran.*
[7]OpenNet Initiative *Internet Filtering in: Pakistan.*
[8]*Ibid.*
[9]OpenNet Initiative *Internet Filtering in: Syria.*
[10]OpenNet Initiative *Internet Filtering in: Sudan.*
[11] Reporters Without Borders - "Internet Enemies", march 2010 http://en.rsf.org/internet-enemie-saudi-arabia,36681.html.

Assabilonline, Reporters Without Borders, and *Al-Jazeera* in Arabic. *Al-Jazeera* in English, however, is still available.[12]

To block child pornography, copyright, or other illegal content, some democratic countries filter Internet content as well. For example, New Zealand has begun maintaining blacklist,[13] and Australia has discussed nation-wide Internet filtering.[14] Denmark and Sweden maintain blacklists for websites suspected of hosting child pornography.[15]

Barriers to Access

Barriers to access can create de-facto restrictions to Internet access. At times, these can be monetary hurdles. For example, ONI reports that in Myanmar "[n]etwork-ready computers must be registered (for a fee)."[16] Additionally, government permission is required if anyone wishes to publish a website.[17] In Cuba, access to the World Wide Web is possible from hotels but at a highly prohibited cost: $6 an hour when the average monthly salary reaches about $20.[18]

Data speeds can be controlled on a national level, limiting access technologically Since 2006, the Ministry of Communications and Information Technology in Iran has maintained an order prohibiting individual Internet access speeds greater than 128 kbps,[19] which can impact an end-users ability to transmit, upload, or view media as well as use communications tools such as Voice over Internet Protocol (VOIP) or video chat. Iran and Burma have both slowed bandwidth speeds during political situations like elections.[20]

Internet connections can also be directly severed for entire regions. For example, following riots in the Xinjiang province in July 2009, the Chinese government cut off Internet access to the

---

[12] Ibid.

[13] John, Ozimek, NZ Internet Filter Goes Live - Gov Forgets To Tell Public, The Register, March 12, 2010, http://www.theregister.co.uk/2010/03/12/new_zealand_internet_filter/.

[14] Jennifer Dudley-Nicholson, Australia's compulsory internet filtering 'costly, ineffective', AustralianIT, October 29, 2008 http://www.theaustralian.com.au/australian-it/net-filtering-costly-ineffective/story-e6frgan6-1111117891445.

[15] A report found that of the 167 websites on Sweden's list, most no longer existed or were deleted, some did not have illegal content, and only three sites hosted illegal child abuse images. The report notes that two of these sites were known since 2008 and "[a]fter sending an abuse message to the hosting provider in the USA, the websites were removed in less than 30 minutes. This suggests that the police did nothing to shut these sites down for about two years. verified that these domains were blocked in Denmark on 28 September 2010, 14:20 GMT+0200 (Central European Summer Time). See *Blacklists of Denmark and Sweden analysed (preliminary version) Analysis of domains blocked in Denmark on 28 September 2010, 14:20:00 GMT+0200 (CEST)*, AK Zensur, *available at*: http://ak-zensur.de/2010/09/29/analysis-blacklists.pdf.

[16] Open Net *Internet Filtering in: Myanmar (Burma).*

[17] *Ibid.*

[18] Reporters Without Borders - "Internet Enemies", march 2010 http://en.rsf.org/internet-enemie-cuba,36678.html.

[19] OpenNet Initiative *Internet Filtering in: Iran,* 7.

[20] Reporters Without Borders "Junta uses Internet upgrade to centralize and reinforce online controls", nov. 10, 2010 http://en.rsf.org/burma-junta-uses-internet-upgrade-to-10-11-2010,38784.html.

province for six months as well as other forms of communication such as text messaging and international phone calls.[21]

Attempts by democratic governments to transition legal frameworks to the digital domain can also create barriers to access. While these barriers may be unintended, they can impact the free flow of information. For example, in May 2010, a German court ruled users were required to password protect their wireless networks.[22] While intended to guard against illegal downloads, the policy can hamper attempts to create community wireless networks.

Mandating User Disconnection

Some countries have viewed disconnecting users from the Internet as solution to copyright infringement, proposing or passing laws that require ISPs to terminate the Internet connection to a home if user is accused of transferring copyrighted material three times. In France, the law "Création et Internet" creates a new agency, *Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet*, to maintain a blacklist of accused households. A household is blacklisted and cut off from Internet access from any ISP for three months to a year after three accusations.[23] Ireland has followed with similar legislation.[24] Similar language recommending all countries follow suit was removed from a draft release of the Anti-Counterfeiting Trade Agreement released in April 2010.[25]

State-enabled Intermediary Censorship

With many emerging modes of communication, the government is not the only entity positioned to engage in censorship activity. A variety of players are involved in accessing and sharing information on the Internet. From Internet Service Providers (ISPs) to blog hosting websites, these intermediaries exist at points in the network at which the flow of information can be restricted or controlled. Whether intentional or unintentional, government policies create and shape the markets that enable or prevent, or even encourage or discourage, such activity. For example, policy frameworks that create broad legal liability on intermediaries and mandate responsibility for content, such as content traversing on a network or posted on a website, create

---

[21]Rebecca MacKinnon *Networked Authoritarianism in China and Beyond: Implicatoins for Global Internet Freedom*, presented at Liberation Technology in Authoritarian Regimes, October 11-12, 2010

[22]Kirsten Grieshaber, *German court orders wireless passwords for all, Associated Press via MSNBC*, May 12 2010, http://www.msnbc.msn.com/id/37107291/ns/technology_and_science-security/ (accessed November 10, 2010.)

[23] Nate Anderson, French anti-P2P Law Toughest in the World, Ars Technica, March 10, 2009,http://arstechnica.com/tech-policy/news/2009/03/french-anti-p2p-law-toughest-in-the-world.ars (accessed April 22, 2010).

[24] Nate Anderson, Major Labels Go *Bragh*? Irish Judge Allows 3 Strikes, Ars Technica, April 2010, http://arstechnica.com/tech-policy/news/2010/04/major-labels-go-bragh-as-irish-judge-allows-3-strikes.ars?utm_source=rss&utm_medium=rss&utm_campaign=rss (accessed April 22, 2010).

[25]*See* Consolidated Text Prepared for Public Release Anti-Counterfeiting Trade Agreement, http://www.ustr.gov/webfm_send/1883.

pressures and incentives to monitor and restrict information.[26] As the Center for Democracy and Technology has found, intermediary liability leads to the self-censorship of information.[27]

Mandating ISP blockage

The responsibility for filtering content can be delegated by a state to network operators. For example, the Chinese government requires ISPs to block specific websites and monitor the activities of users. ONI reports "ISPs are required to record important data (such as identification, URLs visited, length of visit, and activities) for all their users for at least 60 days."[28] ISPs also must monitor and ensure that no illegal content is hosted on servers.[29] A similar law in Iran, the Bill of Cyber Crimes' Sanctions ratified in 2008, "requires ISPs to ensure that 'forbidden' content is not displayed on their servers."[30]

Internet Intermediaries

Web services, such as hosting or search services, represent additional points where intermediary liability can restrict the flow of information. For example, according to Human Rights Watch, all Internet content providers in China, such as websites that host news or blogs, are responsible for all content hosted on the website regardless of author.[31] Rather than government defined lists, these websites each maintain their own lists of banned keywords. In testing keyword sensitivity of 15 different blog hosts in China Rebecca MacKinnon found sites removing content related to such subjects as the Olympics, corruption, and Tibet. [32]

Websites that host video can also be subject to liability. For example, ONI reports that the Chinese government warned web hosting site Tudou.com for "hosting improper videos" in March 2008.[33]

In democracies, policies intended to protect privacy or children can also result create pressures on intermediaries for example, Google was targeted in Italy for a video a user uploaded to YouTube depicting an individual with Down syndrome being bullied. In 2010, three Google executives were convicted and sentenced to six-month suspended sentences for the video.[34]

---

[26] *Organization for Economic Co-Operation and Development (OECD), The Economic and Social Role of Internet Intermediaries, April 2010.* http://www.oecd.org/dataoecd/49/4/44949023.pdf

[27] *Ibid.*

[28] OpenNet Initiative *Internet Filtering in: China, 15*.

[29] *Ibid.*

[30] OpenNet Initiative *Internet Filtering in: Iran*.

[31] "Race to the Bottom" Corporate Complicity in Chinese Internet Censorship" Human Rights Watch

[32] Rebecca MacKinnon, *China's Censorship 2.0: How Companies Censor Bloggers*, First Monday, 2 February 2009

[33] OpenNet Initiative *Internet Filtering in: China, 15*.

[34] Manuela D'Alessandro, Italy Convicts Google Execs for Down Syndrome Video, Reuters via Wired, February 24, 2010

Device Control

Even if government policies are not overtly restrictive, the lack of adequate consumer protections can result in allowing companies pursue business practices that restrict the flow of information. One example in the United States is how network operators restrict network access to a limited set of devices and can affect the types of information that can flow on the network. Prior to the 1968 *Carterfone* decision users in the United States were prohibited from attaching "foreign attachments" – telephones and other equipment made by manufacturers other than AT&T – to the AT&T network. After *Carterfone*, when devices such as fax machines to dial-up modems were allowed to connect, communication and transmission of information was revolutionized.

Despite *Carterfone*, users in the United States remain limited in their use of mobile networks and mobile devices. Mobile operators increasingly prevent user modifications that can unlock additional features such as tethering or open application choice. Sometimes called "jailbreaking" or "rooting," modifying the software on a device has been granted a fair-use exemption by the U.S. Copyright Office.[35] Devices are increasingly being designed to make this practice difficult.[36] For example, the Motorola Android-based phone, the Droid X, contained an "eFuse", a piece of software that renders the device inoperable if any unauthorized software is detected. The T-Mobile G2 phone with Google stored "some components in read-only memory," rolling-back user modifications to the software.[37] Although savvy individuals find solutions to barriers like these,[38] locking down devices and software creates barriers to communication.

Short Codes

Short codes are another a clear example of restrictive behavior by wireless network operators in the United States, unintentionally facilitated by the government. Short codes are five or six character numbers that can allow organizations to easily communicate with individual people using text messages. Through short codes, these groups can disseminate information or updates on business or policy matters of value to their opt-in users. Unfortunately, the process of acquiring and deploying a short code takes place in a messy and complicated market with lax government oversight. Small organizations, including many nonprofits, go through facilitating organizations that specialize in short code campaigns and other outreach technologies. These facilitators must then go through professional short code aggregators, which establish relationships with each individual wireless company in order to unify the phone numbers used in the campaigns.

---

[35] David Kravets, U.S. Declares iPhone Jailbreaking Legal, Over Apple's Objections, Wired, July 26, 2010, http://www.wired.com/threatlevel/2010/07/feds-ok-iphone-jailbreaking/ (accessed: October 11, 2010).

[36] The exceptions granted by the Copyright Office also are limited to the act of rooting or jailbreaking the phone and do not extend to trafficking in devices or software that would allow less sophisticated users to perform the same tasks.

[37] *See* T-mobile press release: http://press.t-mobile.com/articles/t-mobile-G2-code-level-modifications

[38] Elizabeth Fish, The 'Unrootable' G2 Meets its Match, Gets Hacked, PC World, November 11, 2010, http://www.pcworld.com/article/210430/the_unrootable_g2_meets_its_match_gets_hacked.html (accessed: November 13, 2010).

This complicated market has exhibited numerous examples of censorship. In the earliest widely publicized incident, Verizon Wireless refused to permit an abortion rights group, NARAL Pro-Choice America, to use its short code to communicate with interested opt-in users on policy issues.[39] Verizon's rationale was that the company did not wish to allow its customers to receive messages from any organization "that seeks to promote an agenda or distribute content that... may be seen as controversial or unsavory to any [Verizon] users." After substantial media pressure, Verizon reversed its decision, but not after causing significant harm and expense.

Regardless of the company's motives, Verizon's action constituted deliberate censorship of political speech and organizing activity, enabled by lax government oversight. Despite being built on top of text messages, a service well within the purview of the Federal Communications Commission's oversight over all communications by wire or radio, neither short codes nor text messages themselves have ever been classified or subject to government oversight by the FCC. A petition was filed in 2007, on the heels of Verizon's act of glaring censorship, to ask the FCC to classify these services and to exercise rulemaking authority to prevent similar abuses going forward.[40] The FCC has failed to act on this petition, leaving text messaging and short codes in a state of legal limbo.

The result of government inactivity has been the continued existence of a market that enables pervasive censorship. In the spring of 2010, Sprint threatened to discontinue a short code in use by Catholic Relief Services to help connect interested individuals to a call center to learn more about disaster relief efforts in Haiti.[41] In the fall of 2010, T-Mobile prevented the use of a short code by a California medical marijuana dispensary listing service.[42] Although it's unclear whether or to what extent censorship in short codes is done out of a desire to censor content - for example, it seems unlikely that Sprint would have wanted to inconvenience Catholic Relief Services on the basis of the group's substantive message - the impact and the effect of censorship is significant and harmful regardless of its underlying motive. On the one hand, this censorship exists in some part because of government action in allocating spectrum and shaping wireless markets that give rise to short code services that enable censorship of political speech and activity. On the other hand, the censorship occurs in larger part due to government inaction - the failure of the government to take a meaningful role in protecting the open flow of information and speech.

---

[39] Adam Liptak, *Verizon Blocks Messages of Abortion Rights Group*, New York Times, September 27, 2007 http://www.nytimes.com/2007/09/27/us/27verizon.html

[40] Petition for Declaratory Ruling of Public Knowledge, Free Press, Consumer Federation of America, Consumers Union, EDUCause, Media Access Project, New America Foundation, U.S. PIRG, Dec. 11 2007, http://www.publicknowledge.org/node/1303

[41] http://www.nytimes.com/2010/03/25/technology/25texting.html

[42] http://www.wired.com/threatlevel/2010/09/text-message-censorship/

Discriminatory Networks

Networks are the conduits for the flow of information but information over these networks is not always treated equally. Whereas a government can actively restrict the free flow of information by using filtering technology, government policies can enable network operators to create restrictions for their own financial gains when open network requirements are not in place. Commonly referred to as Network Neutrality, the principle requires network operators to treat all traffic equally and not discriminate against any content, application, or service.

One infamous example of a non-neutral network occurred in the United States in 2007 when Robb Topolski noticed that his BitTorrent file transfers of public domain music were consistently failing. After troubleshooting, Topolski discovered that Comcast, his ISP, was intercepting packets sent from his computer and inserting RST packets that caused his connections to reset.[43] In Europe, several ISPs restrict video, VoIP, or peer-to-peer protocols. Other examples of non-neutral networks include restricting access to websites, such as UK ISP BT blocking access to the Pirate Bay website in 2009,[44] or Canadian company Telus blocking access to the website of the Telecommunications Workers' Union of Canada in 2005.[45] Mobile network operators also limit traffic by blocking specific applications such as VoIP or the ability to share the network connection with other devices, also known as tethering.

Neither the Federal Communications Commission in the United States nor the European Commission in Europe has acted to preserve neutral networks. Canada introduced rules in 2009.[46]

3. Trade Agreements

The Internet facilitates business by enabling new forms of communication while introducing new markets and innovations. Trade policy is one lever that can impact how the Internet operates as a global network. While we have described a range of Internet restrictions, these methods for explicit political censorship can also inherently block access to domestic markets and potentially protect the market interests of incumbents.[47]

---

[43] Peter Eckersley, Fred von Lohmann and Seth Schoen, *Packet Forgery By ISPs: A Report On The Comcast Affair*, November. 2007,) *available at:* www.eff.org/files/eff_comcast_report2.pdf.

[44] Barry Collins, *BT Blocks off Pirate Bay*, PC Pro, 21 April 2009, *available at:* http://www.pcpro.co.uk/news/251609/bt-blocks-off-pirate-bay.

[45] http://boingboing.net/2005/07/24/phone-company-blocks.html

[46] Canadian Radio-television and Telecommunications Commission, *Review of the Internet Traffic Management Practices of Internet Service Providers*, Telecom Regulatory Policy CRTC 2009-657, 21 October, 2009), *available at*: http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm.

[47] Tim Wu, *The World Trade Law of Internet Filtering* (May 3, 2006). Available at SSRN: http://ssrn.com/abstract=882459.

However, trade agreements can also threaten the flow of Information and create challenges in addressing other policy objectives. For examples, some leaked drafts of the Anti-Counterfeiting Trade Agreement (ACTA) have revealed provisions that work against freedom of expression and create barriers to innovations or new technologies. One such provision proposed restricting Internet access of households accused of infringing copyright,[48] creating an imbalanced policy framework that leaned towards reducing access to information. Another provision, present even in a draft recently released by the United States Trade Representative,[49] proposes to block user attempts to circumvent Digital Rights Management (DRM).[50] Devices such as cell phones can be locked by manufacturers and carriers to prevent some functionality. For example, when the first cell phones with cameras were released in the United States, users were forced to pay for compounded fees in order to transfer the images to a computer,[51] and VoIP applications were also initially blocked from cellular networks.[52] While users' right to change software on their phone or unlock additional features has been upheld in the United States,[53] an international level ban on circumvention of DRM could greatly restrict how information is captured and shared.

Additionally, restrictions on the flow of information on the Internet through trade agreements can create additional challenges for other U.S. policy objectives. Trade agreements do not guarantee a holistic approach to Internet openness, and any restrictions created through them will be interpreted differently by nations that have strong civil rights and freedom of expression frameworks and those that do not. Provisions that limit access to the Internet, monitor communications, or restrict the flexibility of software or devices to can create justifications for additional restrictions particularly in nations whose civil frameworks encourage censorship.

4. Effects on the flow of information

Additional Restrictions on the Individual

For the individual, the examples of restrictions described in these comments create barriers to communicate or access information. The above examples of restrictions implemented by government or network operators demonstrate a range of ways, from blocked websites to locked-down communications technology websites, in which individuals face restricted flows of information, access to innovations, and the ability to tell their story.

---

[48] Anti-Counterfeiting Trade Agreement, Informal Predecisional/Deliberative Draft, (January 18, 2010), http://www.laquadrature.net/files/201001_acta.pdf

[49] The Anti-Counterfeiting Trade Agreement, (November 15, 2010), http://www.ustr.gov/webfm_send/2379

[50] http://www.michaelgeist.ca/content/view/5285/125/.

[51] Tim Wu, *Wireless Net Neutrality: Cellular Carterfone and Consumer Choice in Mobile Broadband,* New America Foundation Working Paper #17, February 2007.

[52] Stacey Higginbotham, Apple Brings 3G VoIP to the iPhone, GigaOM, January 28, 2010, http://gigaom.com/2010/01/28/apple-brings-3g-voip-to-the-iphone/

[53] David Kravets, U.S. Declares iPhone Jailbreaking Legal, Over Apple's Objections, Wired, July 26, 2010, http://www.wired.com/threatlevel/2010/07/feds-ok-iphone-jailbreaking/ (accessed: October 11, 2010).

However, policies can also create a culture of self-censorship. As Wendy Seltzer writes "overbroad 'subversive activities' law" can have a chilling effect where individuals err on the side of precaution.[54] Seltzer cites *Drombrowski v. Pfister*: "The chilling effect upon the exercise of First Amendment rights may derive from the fact of the prosecution, unaffected by the prospects of its success of failure."[55] Overly broad or ambiguously defined laws for acceptable behavior, particularly when combined with deification requirements, can create chilling effects – and examples can be found in a growing number of countries. For example in South Korea, websites with over 100,000 visitors must verify the real names of users, resulting in the investigation and even prosecution of Internet users who spoke critically of the government and who would otherwise have remained anonymous – or at very least much more difficult to trace.[56] Internet cafe operators in Syria must record the names, identification cards, and times of use of their customers.[57] In China, users must register with real names for the use of some services,[58] and cyber cafes, popular among lower income populations, monitor users through cameras and through software installed on the computers.[59] Last May, the Chinese minister of the State Council Information Office, said the authorities were "exploring an identity authentication system" for users of online forums. Internet users are currently required to register before posting comments on these site but they can use a pseudonym to post. Wang said that, after preventing anonymous posting on major news portals and commercial websites, the aim now was to extend the system to online forums and chat websites.[60]

On 29 April 2010, the Chinese parliament passed an amendment to the State Secrets Law forcing Internet and telecommunications companies to cooperate closely with the authorities on matters relating to national security.[61] In China, computers are sold with "Green Dam Youth Escort," software that has been found to censor political and religious content as well as monitor user

---

[54] Wendy Seltzer, *Free Speech Unmoored in Copyright's SafefHarbor: Chilling Effects of the DCMA on the First Amendment*, The Berkman Center for Internet & Society Research Publication Series, March 2010.

[55] 380 U.S. 479, 488-89 qtd. in Wendy Seltzer, *Free Speech Unmoored in Copyright's SafefHarbor: Chilling Effects of the DCMA on the First Amendment*, The Berkman Center for Internet & Society Research Publication Series, March 2010.

[56] *Access-Controlled Country Profile: South Korea*, http://www.access-controlled.net/wp-content/PDFs/part2/028_South%20Korea.pdf

[57] OpenNet Initiative *Internet Filtering in: Syria*

[58] OpenNet Initiative *Internet Filtering in: China*

[59] Rebecca MacKinnon *Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom*

[60] Reporters Without Borders - "Authorities turn their sights on microblogging", July 26th, 2010 - http://en.rsf.org/china-authorities-turn-their-sights-on-16-07-2010,37971.html

[61] Reporters Without Borders, may 7th, 2010 "Government crusade against online anonymity" http://en.rsf.org/china-government-crusade-against-online-07-05-2010,37412.html

data.[62] Though initially required on all computers, China has since softened requirements on foreign manufacturers to install the software, although efforts continue to require the installation of monitoring and filtering software on devices deployed at the institutional level.[63]

Restrictions on Groups

Policy environments can create barriers for groups seeking to organize around political issues or communications. From blocked content on websites to limited modes of communications, various Internet restrictions can result from direct government control or but also lack of protections that support the free flow of information. For example, direct control was demonstrated by Iran in blocking access to Facebook and Twitter before elections in 2009. [64] Direct control can be exemplified by policies that create norms of allowable or censored speech, such the Chinese government driving blog hosting websites to block a range of content based on regular censorship requests from several government departments. Device or protocol limitations can also create barriers, such as China blocking calls from VoIP to telephone calls.[65]

While likely not the intention of government policies, lack of protections can also result companies placing restrictions on groups. For example the lack of requirements for network operators to maintain neutral networks enabled Telus to block access to the Telecommunications Workers' Union of Canada website in 2005.[66] Additionally, T -mobile blocked access to Truphone in the UK before the government stepped in to protect consumer communications.[67]

Restrictions on Innovators

Restrictions to networks can create challenges for innovators to bring new products to market. On a neutral network, packets of data is transmitted been users across and between networks on a non-discriminatory framework. Any type of information is able to pass and the network neither promotes nor hinders any particular application or content. Neutral networks allow for an open Internet layer and low barriers to entry for new ideas and innovations and insulate competition among applications and services from market incentives of the network layer.[68] As Riley and

---

[62] Rebecca MacKinnon *Networked Authoritarianism in China and Beyond: Implications for Global Internet Freedom*, presented at Liberation Technology in Authoritarian Regimes, October 11-12, 2010

[63] Rebecca MacKinnon, *Testimony submitted for the Record for the Hearing "Google and Internet Control in China,* Congressional-Executive Commission on China, March 24, 2010.

[64] Ali Sheikholeslami, Iran Blocks Facebook, Twitter Sites Before Elections (Update1) , Bloomberg, May 23, 2009, http://www.bloomberg.com/apps/news?pid=newsarchive&sid=anh.uW3gNZp4

[65] Guy Kewney, China Blocks Skype, VoIP, The Register, September 12, 2005, http://www.theregister.co.uk/2005/09/12/china_blocks_skype/

[66] *Telus cuts subscriber access to pro-union website*, CBC News, July 24, 2005, http://www.cbc.ca/canada/story/2005/07/24/telus-sites050724.html

[67] Bill Ray, T-Mobile forced to connect Truphone numbers, The Register, 17 July 2007, accessed 5 November 2010

[68] *See* Brett Frischmann & Mark Lemley, "Spillovers", 107 Colum.L.Rev. 257 (2007);.and Lawrence Lessig *The Future of Ideas: The Fate of the Commons in a Connected World* (Vintage, 2002,) 46-47.

Topolski explain, the "performance of an application or service online as compared to its competitors is determined by the design and engineering of the application or service."[69]

However, when networks are not neutral and discriminate or place restrictions on the traffic of an application or service, network operators, acting in their own interest or that of the State, are able to operate as a gatekeeper, controlling information or applications over the network. Riley and Topolski use a hypothetical scenario of RealPlayer and YouTube:

> "Imagine if RealVideo, the video format used in RealPlayer, was classified as a priority application upon its original release in 1997. Upon its introduction in 2005, YouTube might not have received the same level of priority, because it uses a fundamentally different protocol and business model--YouTube hosts video itself, whereas RealVideo is hosted on individual websites. After eight years of prioritized use, the video quality of RealVideo would have held a substantial advantage over the new entrant, YouTube, which would be effectively degraded by the imposition of priority for RealPlayer. YouTube would have faced an uphill battle to adoption, being required to compete as a video service without priority; it might well have failed, while on a level playing field, it flourished."[70]

Additionally, as Barbara van Schewick explains integrating network layers reduces the flexibility inherent to the Internet: "[i]n an integrated architecture, it is usually not possible to make changes to a component that do not trigger changes in the rest of the system."[71] Network based blocking of content, restrictions on speed, or discrimination against applications can all create barriers to innovators attempting to introduce new applications and services.

5. Recommendations for preserving openness

The issues raised in this proceeding are broad, and span many agendas and agencies across, both domestic and international implications. This proceeding affects those who preserve individual human rights and free expression, as well as those who strive for responsible economic policies. Free and open information flow matters as much for culture as it does for free trade, as much for democracy as for intellectual property. An open Internet created by an open, global flow of information provides both the host forum and the access mechanism for all of these activities, and consequently, a diverse range of agendas is implicated by any harm to this flow.

Promoting the global free flow of information is broader than any small set of specific policy actions. While it is important to address governments that engage in direct harmful censorship, it

[69]M. Chris Riley and Robb Topolski, "The Hidden Harms of Application Bias," Free Press/New America Foundation Policy Brief, November 2009, 6, available at: http://www.newamerica.net/publications/policy/the_hidden_harms_of_application_bias

[70]M. Chris Riley and Robb Topolski, "The Hidden Harms of Application Bias," Free Press/New America Foundation Policy Brief, November 2009, 6, available at: http://www.newamerica.net/publications/policy/the_hidden_harms_of_application_bias

[71]Barbara van Schewick *Internet Architecture and Innovation*, (Cambridge: MIT Press, 2010,) 125.

is also important to consider how other policies can result in restrictions on the part of companies. This proceeding is about whether government policies create an environment that promotes the free flow of information or enables and incentivizes restrictions. Between different nations, a pro-information approach is not a drag-and-drop policy framework but one that creates an environment promoting access to information.

Pro-information policy can be defined by government inaction – such as not actively censoring information or conducting surveillance – or by government action – preventing censorship by foreign governments or private corporations, and strengthening safe harbors that protect intermediaries from being required or encouraged to participate in censorship activity.

With respect to the NTIA, a pro-information policy requires a comprehensive, and unified, approach throughout the executive branch and independent agencies, both domestically and internationally.[72] Pro-information policy must be a calculation in how United States approaches economic policy, trade, telecommunications, crime, education, health, and many other areas.

Commenters encourage the NTIA to support pro-information policy in all its activities, beginning, but not ending with the current active initiatives in the Department of Commerce, and extending into the NTIA's advisory role for other federal agencies.

Respectfully submitted,

/s/

James Losey
Rebecca MacKinnon
Benjamin Lennett
Open Technology Initiative
New America Foundation

M. Chris Riley
Free Press

Eddan Katz
Electronic Frontier Foundation

Rashmi Rangnath
Public Knowledge

[72] Cases of blocking access to information, such as seizing data of journalistic endeavors such as Indy media serve as poor examples for U.S. domestic policy. *See* https://w2.eff.org/Censorship/Indymedia/.

Clothilde Le Coz
Reporter Without Borders

Jay Stanley
American Civil Liberties Union