The No-Nonsense *guide to*

The Great Internet Grab

Who wins, who loses?

WACC

January 2012

Controlling or restricting access to or the publication of information on the Internet amounts to censorship. It may be done by governments or by private organizations either at the behest of government or on their own initiative. However, organizations and individuals may also engage in self-censorship on their own or due to intimidation and fear. The question is: What restrictions, if any, should be placed on the Internet?

The issues surrounding Internet censorship are similar to those related to more traditional media such as newspapers, magazines, books, music, radio, television, and films. One difference is that national borders are more permeable online: residents of a country that bans certain information can find it on websites hosted outside their country. Thus censors must work to prevent access to information even though they lack physical or legal control over the websites themselves. This in turn requires the use of technical censorship methods that are unique to the Internet, such as site blocking and content filtering.

Control is not limited to filtering or plain censorship. Recent years have seen an increase in a wide variety of threats to Internet freedom, such as the arrest of bloggers and Internet users. The Committee to Protect Journalists (CPJ) found that in 2008, for the first time, there were more jailed "cyber-dissidents" than traditional media journalists. The arrest or detention of content producers (such as journalists or bloggers), or users (such as those who are accessing or consuming unlawful or otherwise targeted material) is one of the most traditional forms of content control. In doing so, surveillance and monitoring methods are often used to identify users or producers.

One of the four winners of the CPJ's 2011 International Press Freedom Awards was Natalya Radina, editor-in-chief of the pro-opposition news website Charter 97 in Belarus. In December 2010 she was arrested by the country's security services following post-election opposition protests in Minsk. She was indicted on charges of organizing mass disorder and faced up to 15 years in prison Radina was released, pending trial, and forced to relocate from Minsk to the town of Kobrin, where her movements were restricted and she was ordered to check in daily with authorities. Unable to work and fearing imprisonment, she fled Belarus for Russia, where she spent months in hiding. She was later granted asylum in Lithuania, where she continues to edit Charter 97.

Internet censorship practices

Once upon a time it was assumed that states could not control Internet communications. Today, according to the OpenNet Initiative [http://opennet.net], more than 40 countries engage in Internet censorship. Those with the most pervasive filtering policies have been found routinely to block access to human rights organizations, news, blogs, and web services that challenge the status quo or are deemed threatening or undesirable. Others block access to single categories of Internet content, or intermittently to specific websites or network services to coincide with strategic events, such as elections or public demonstrations.

Some States enact Internet filtering legislation, most with little or no transparency and public accountability. Most States do not reveal what information is being blocked, and only rarely are there review or grievance mechanisms for affected citizens or content publishers. Compounding the problem is the increasing use of commercial filtering software, which is prone to overblocking due to faulty categorization. Commercial

filters block access to categorized lists of websites that are kept secret for proprietary reasons. As a consequence, unaccountable private companies determine censorship rules in political environments where there is little public accountability or oversight.

In 2006, Reporters without Borders (Reporters sans frontières, RSF), began publishing a list of "Enemies of the Internet". An enemy of the internet is one marked not just for its capacity to censor news and information online but also for its almost systematic repression of Internet users. In 2007 a second list of countries "Under Surveillance" was added. Both lists are updated annually.

When "Enemies of the Internet" was started, it named 13 countries. By 2011 the number of countries had fallen to 10 with the move of Belarus, Egypt, and Tunisia to "Countries under Surveillance". When that list started in 2008, it named 10 countries. By 2011 the number of countries had grown to 16.

In the 2011 edition of Freedom House's report *Freedom on the Net*, of 37 countries surveyed, 8 were rated as "free" (22%), 18 as "partly free" (49%), and 11 as "not free" (30%). That same year, UNESCO's Division for Freedom of Expression, Democracy and Peace commissioned the report *Freedom of Connection, Freedom of Expression. The Changing Legal and Regulatory Ecology Shaping the Internet*, written by William H. Dutton, Anna Dopatka, Michael Hills, Ginette Law, and Victoria Nash (UNESCO, 2011). The authors stated:

> "Freedom of expression and the right to communicate are, in many ways, being redefined by the development of and access to new technologies. Modern progress on the Internet challenges, yet also enables, freedom of expression. Today we see the emergence of two types of filtering variously applied in different nations and regions of the world: 1) filtering for the protection of other citizen values, such as privacy or child protection; and 2) filtering to impose a particular political or moral regime, such as is entailed in governmental surveillance or political repression."

In tandem with advances in technology underpinning greater access to the Internet, social media and mobile communication technologies, there have been innovations in technological approaches to controlling the flow of information over these networks. This has been driven by the need to maintain and improve the quality and security of services, such as by screening out spam email and viruses, but also by efforts to block unwanted content as judged by individuals, parents, NGOs, corporations or governments. Regulation of Internet content is enabled by technologies that

SOPA and PIPA

The Stop Online Piracy Act (SOPA) is a bill introduced by U.S. Representative Lamar S. Smith (R-TX) to expand the ability of U.S. law enforcement to fight online trafficking in copyrighted intellectual property and counterfeit goods. Provisions include the requesting of court orders to bar advertising networks and payment facilities from conducting business with infringing websites, and search engines from linking to the sites, and court orders requiring Internet service providers to block access to the sites. A similar bill in the U.S. Senate is titled the PROTECT IP Act (PIPA).

Proponents of the legislation state it will protect the intellectual-property market and corresponding industry, jobs and revenue, and is necessary to bolster enforcement of copyright laws, especially against foreign websites. Claiming flaws in present laws that do not cover foreign-owned and operated sites and citing examples of "active promotion of rogue websites" by U.S. search engines, proponents assert stronger enforcement tools are needed.

Opponents state the proposed legislation threatens free speech and innovation, and enables law enforcement to block access to entire internet domains due to infringing content posted on a single blog or webpage. They have raised concerns that SOPA would bypass the "safe harbor" protections from liability presently afforded to Internet sites by the Digital Millennium Copyright Act. Library associations have expressed concerns that the legislation's emphasis on stronger copyright enforcement would expose libraries to prosecution. Other opponents state that requiring search engines to delete a domain name could begin a worldwide arms race of unprecedented censorship of the Web and violates the First Amendment.

On January 18, 2012, a series of coordinated protests occurred against SOPA and PIPA. These followed smaller protests in late 2011. Protests were based on concerns that the bills, intended to provide more robust responses to copyright infringement (colloquially known as piracy) arising outside the United States, contained measures that could cause great harm to online freedom of speech, websites, and internet communities.

The move to a formal protest was initiated when some websites, including Reddit and the English Wikipedia's community of editors, considered temporarily closing their content and redirecting users to a message opposing the proposed legislation. Others, such as Google, Mozilla, and Flickr, soon featured protests against the acts. Some shut completely, while others kept some or all of their content accessible. In all, over 115,000 websites and unknown tens of millions of individuals joined the internet protest.

can be used at different levels.

As information and communication goes online, it may use several Internet-related protocols and services, passing through various points in the Internet network as well as the end user's device. As a result, filtering methods can be applied at various points throughout the network. Most concern is focused on State- or government-sponsored or enforced filtering, but even when State-mandated, it can happen at different levels and be done by various different parties such as individuals, institutions and service providers. Generally, those concerned about the civil liberties of Internet users want filtering decisions to be made at the lowest possible level – as close as possible to the individual user.

Alternatives to filtering

Government agencies have used a number of other techniques to prevent access or to censor particular types of content. These include:

- Denial of service attacks, which produce the same end result as other technical blocking techniques – blocking access to certain websites – although only temporarily.
- Restricting access to domains or to the Internet, such as by installing high barriers (costs, personal requirements) to register a domain or even to get Internet access.
- Search result removals, by which search engine providers can filter web content and exclude unwanted websites and web pages from search results. By using blacklists, parsing content and keywords of web pages, search engines are able to hinder access.
- Taking down websites (removing sites from servers), is one of the most effective ways of regulating content. To do so, regulators need to have direct access to content hosts, or legal jurisdiction over the content hosts, or an ability to force Internet Service Providers (ISPs) to take down particular sites. In several countries, where authorities have control of domain name servers, officials can deregister a domain that is hosting restricted content.

Controlling the Internet is a fundamental aspect of Internet politics and most countries have viewed some level of censorship as a legitimate means to protect a nation's interest, such as in online child protection. However, the degree and nature of legitimate targets of online censorship can vary significantly, depending on the actor, and the cultural or political character of the state in which it occurs. The transparency and implementation of government policy is a key problem here. Often, it is not clear from policy statements and law to what extent access to Internet material is blocked.

It is often thought that content control systems are only established in undemocratic countries or by authoritarian regimes wishing to control political speech or criticism. In fact, content control measures have become more prevalent around the world and are often undertaken for a wide variety of reasons, often with very good intentions. In democratic societies, issues of copyright infringement, hate speech, defamation, privacy protection, and child protection are at times a basis for Internet filtering or other content control.

Clearly it could be argued that filtering for such purposes does not represent as significant a threat to freedom of expression as the deliberate blocking of political speech or information and communication for certain social minority groups. Others, who see freedom of expression as an absolute right of fundamental importance, might disagree.

Child protection

The Internet is an increasingly central component in the lives of children and young people in the developed world. It cannot be seen as an "adults-only" environment. It is in this context that some of the most emotive debates around freedom of expression online arise, at the point where the crucial regulatory goal of preventing harm to minors pushes up against the noble ideal of free speech for all. Many, possibly even most states, have introduced some regulatory tools to protect children online, at least in terms of prohibiting illegal activity; the question remains as to how much regulation is enough, and how much is too much. In many jurisdictions, this debate hinges in large part on the distinction between activities that are illegal and those that are harmful.

How can the Internet's infrastructure be employed to create an environment where government regulation can be efficient and effective without also being an unreasonable burden? The Montevideo Memorandum (2009) promotes a set of standards for Latin American countries and is one example of a regulatory framework that seeks a balance between guaranteed rights for children, and protecting them from online risks.

No matter where governments decide to limit freedom of expression rights in the name of child protection, it is important that such regulation be transparent, focuses on specific potential risks, and is measured by its effectiveness. In doing so, governments can employ tools to protect the most vulnerable while lessening risks that their efforts be perceived as tools of a broader repression of speech.

In 2009 the Canadian Centre for Child Protection (CCCP) launched a Respect Yourself public awareness campaign designed to teach teens about the risks they face when sending pictures or videos by email, instant messaging or by posting them online. "Children need to fully understand the ramifications of sending pictures or videos, because once they send it, they no

longer have control over who sees it or what is done with it from that point on," said Lianna McDonald, CCCP's Executive Director.

Launched on Safer Internet Day – an internationally recognized day to promote the safe and responsible use of online and mobile technology – the Respect Yourself campaign included a comprehensive website for teens, a Respect Yourself booklet distributed to more than 300,000 grade seven students across Canada, and a series of three posters for use inside classrooms.

Case study: Google and China[1]

In 2010, Google was the world's most popular Internet search company, maintaining offices in dozens of countries and offering search results in over 100 languages. The corporation has been clear on issues of freedom of expression: Google's stated mission is "to organize the world's information and make it universally accessible and useful." Nevertheless, Google has faced requests to remove or restrict information from many countries, including Brazil, Germany, India and the US, and seeks to comply fully or partially.

From time to time, Google's decisions have stirred up controversy. The most notable example of this involved its relationship with China. Until 2006, Google had no headquarters with employees in China. However, it provided a Chinese-language version of Google.com that was easily accessible to users in China. In 2002, China began blocking access within the country to Google's servers.

Google faced more problems over the next three years when access was sporadically blocked or slowed and it became clear that the Chinese government was filtering search results. Google users found requests were often denied or redirected to other search engines operating within China and were subject to strict censorship requirements.

Facing such difficulties, and losing market share to their major competitor, Baidu, Google decided in early 2006 to reverse its stance against self-censorship. It opened offices in China and began operating Google.cn. In doing so, it committed itself to respecting the content restrictions imposed by Chinese law and regulations, as it does in other countries in which it operates.

Google continued to auto-censor results on Google.cn until January 2010 when the search engine announced that the company, along with at least 20 other large corporations, had faced sophisticated cyber-attacks originating from within China. These attacks led to the theft of intellectual property for and unauthorized access to the email of human rights activists. Consequently, Google announced that it would stop censoring its search results on Google.cn and

Opponents of Internet Censorship

In addition to the thousands of people who combat censorship through blogs every day, there are several organizations that raise awareness about Internet censorship. Some are formal organizations with prestigious memberships, while others are looser groups that aren't above advocating a guerrilla approach to subverting strict policies.

The OpenNet Initiative is a group that strives to provide information to the world about the ways countries allow or deny citizens access to information. The initiative includes departments at the University of Toronto, the Harvard Law School, Oxford University and the University of Cambridge. ONI's Web page displays an interactive map that shows which countries censor the Internet. [http://opennet.net/]

Reporters Without Borders concerns itself with Internet censorship, although the group's scope extends beyond Internet practices. It maintains a list of "Internet enemies", countries that have the most severe Internet restrictions and policies in place [http://en.rsf.org/].

The American Civil Liberties Union (ACLU) is an adamant opponent of Internet censorship. The ACLU has filed numerous lawsuits in order to overturn censorship laws. In 2007, the ACLU convinced a federal court that the Children's Online Protection Act (COPA) was unconstitutional. COPA was a law that made it illegal to present material online that was deemed harmful to minors, even if it included information valuable to adults [http://www.aclu.org/].

OpenMedia.ca is a non-profit organization that safeguards the possibilities of the open and affordable Internet. It works towards informed and participatory digital policy. It is known for co-ordinating Stop The Meter, the largest online campaign in Canadian history, involving nearly half-a-million people. It has proven that the pro-Internet community can come together and make change.

Other groups offer advice on how to disable or circumvent censorware (see, for example, http://www.peacefire.org/. Some advocate using proxy sites. A proxy site is a Web page that allows you to browse the Web without using your own Internet protocol (IP) address. You visit the proxy site, which includes a form into which you type the URL of the restricted sites you want to visit. The proxy site retrieves the information and displays it. Outsiders can only see that you've visited the proxy site, not the sites you've pulled up.

operate an unfiltered search engine, even if that meant closing its offices in China.

Reaction to Google's announcement was mixed. The US Congress announced an investigation into the cyber-attacks. US Secretary of State Hillary Clinton presented a well publicized speech about Internet freedom and made reference to Google's announcement by requesting transparency from the Chinese government. She highlighted that the United States and China had "different views" on the freedom of information online.

The Chinese media responded by accusing Google and the US government of trying to use the Internet to impose Western values worldwide. Links between Google's commercial decision and the politics of freedom of expression were presented by China's People's Daily Online as a move that politicized a commercial decision.

In March 2010, Google stopped censoring its search service. From then on users visiting Google.cn were redirected to Google.com.hk, where Google offers uncensored search results delivered via servers housed in Hong Kong in simplified Chinese. As China's content restrictions do not apply to services in Hong Kong, Google felt that this solution was consistent with Chinese law. China appeared to accept this remedy.

Promoting Net neutrality

Network neutrality is a founding principle of the Internet – net neutrality ensures that network owners (like ISPs) do not favor some content over other content.

With a few small exceptions, it is the de facto standard of non-discriminatory treatment that has governed the traffic of digital information until recently. Outside of limited exceptions such as spam and known viruses, companies that deliver information over the Internet were required to treat all content equally, delivering each package of information as quickly and efficiently as possible. Under this regime, an Internet user is free to use any equipment, content, application or service on a non-discriminatory basis without interference from the network provider. Net neutrality means that the network provider's only job is to move data – not to choose which data to privilege with higher quality service.

Unfortunately, many ISPs like big telephone and cable companies are successfully removing the network neutrality principle. Large telecommunications

companies have expressed the opinion that, in an age of growing bandwidth use, network neutrality is neither feasible nor desirable. These companies are in a position to play gatekeeper: deciding which web sites load fast or slow, and which won't load at all. They have expressed interest in charging content providers to guarantee speedy delivery of their data. They also have the ability to discriminate in favour of their own search engines, Internet phone services, and video streaming services – while slowing down or blocking their competitors.

Instead of a level playing-field, such companies want to reserve express lanes for their own content and services – for those from big corporations that can afford the steep tolls – and leave everyone else in the slow lane. These Internet providers are lobbying government authorities to refrain from applying network neutrality principles to the Internet, as this would close-off enormous revenues from their ownership of the Internet's physical architecture, which they often retain from their history as government funded and protected monopolies.

Without network neutrality protections, the speech of the smallest and least enfranchised will be the most endangered. The people with the fewest resources to pay for access will be the most likely to be relegated to the slow lane. Some of the benefits of Internet communications over traditional media will be lost as the same gatekeepers of the past impose gatekeeping functions on modern communications.

Network neutrality drives economic innovation, democratic participation, and free speech online. Many of today's most successful applications were developed because a neutral playing field allowed them to develop alongside other more dominant players Without some basic protection for net neutrality, an oligopoly of phone and cable companies will be in a position to control the information that travels over the Internet, possibly cutting restrictive deals with the highest bidding companies and shunting aside innovators, small businesses and entrepreneurs.

In this situation, the network operators will be able to choose winners and losers. In a neutral network, users have the power to choose which applications will be successful.

In 2011 WACC drafted the document *Communication for All: Sharing WACC's Principles* in the belief that communication, rooted in ethical principles of truth, fairness and balance, plays a crucial role in tackling questions of peace, security, justice, mutual accountability and responsibility. The document states:

> "The life of a community is enriched by open, honest and transparent dialogue about decisions and events affecting the lives of its members. This applies equally to a neighbourhood or village, a city, a religious community or a community of nations. Relationships within a community are created and strengthened by face-to-face conversation, community media run by and for its members, and social media that enable genuine participation in political, social and cultural questions relating to the common good."

The Internet is part of the common good of today's information and communication societies. As such it should be run honestly, transparently and democratically. ■

Note

1. This section is taken from *Freedom of Connection, Freedom of Expression. The Changing Legal and Regulatory Ecology Shaping the Internet*, by William H. Dutton, Anna Dopatka, Michael Hills, Ginette Law, and Victoria Nash (UNESCO, 2011).

This No-Nonsense Guide *was compiled from a number of sources by Philip Lee and is published by the World Association for Christian Communication (WACC).*

The World Association for Christian Communication (WACC) is an international organization that promotes communication as a basic human right, essential to people's dignity and community. Rooted in Christian faith, WACC works with all those denied the right to communicate because of status, identity, or gender. It advocates full access to information and communication, and promotes open and diverse media. WACC strengthens networks of communicators to advance peace, understanding and justice.

WACC is responsible for the Centre for Communication Rights portal – a source of documents and materials about all aspects of communication rights.
www.centreforcommunicationrights.org

WACC, 308 Main Street, Toronto Ontario M4C 4X7, Canada

WACC, 71 Lambeth Walk, London SE11 6DX, United Kingdom

www.waccglobal.org