Online Freedom of Speech: The Battle Continues

Walid AL-SAQAF

Diplo Foundation Webinar
September 25, 2012

Relevant Questions

1. The UN Human Rights Council's issued a resolution affirming human rights on the Internet. What implications could such a step have?

2. In an attempt to bypass restrictions on freedom of speech, do online users have the right to access the Internet anonymously?

3. Are companies removing content arbitrarily, moving away from justifications that censored content may have broken local laws or terms of service?

4. How could the challenge of Internet censorship be addressed and contextualized when formulating Internet governance policies?

Online Freedom of Expression as a Human Right

- UN resolution (A/HRC/20/L.13) issued on July 6, 2012 includes "promotion, protection, and enjoyment of human rights on the Internet."
- Swedish Foreign Minister Carld Bildt called it *"A Victory for the Internet"*
- Even China backed the resolution but keeps on censoring online speech
- Chinese representative at deliberations stressed the need to restrict freedom
- But the resolution is not binding and is has room for different interpretations
- No way to directly punish or penalize violating nations
- Could merely be used for '*public shaming*' according to Ken Roth of HRW
- Universal Declaration of Human Rights already includes guarantees for freedom
- National laws and some international laws stand in the way
- Context of Arab Spring crucial (Tunisia, Libya, Egypt among backers)

How much work is needed to deal with Internet Censorship?

Mechanisms of Internet Censorship

1) Technical methods :

Objective: Hide online content from Internet user

- Filtering (includes TCP/IP header & content or HTTP proxy filtering)
- DNS Tampering/Hijacking
- Denial of Service (DoS) Attacks
- Server Takedown
- Surveillance
- Search result filtering
- Filtering by blog service providers
- Slowing down speed, causing disconnections for bulk traffic

Mechanisms of Internet Censorship

2) Non-technical methods

Objective: deter producers, disseminators or viewers of online content

- Legal prosecution
- Detention (often illegally)
- Intimidations, threats and other illegal violations
- Surveillance (through cameras, registering, showing IDs, etc.)
- Social and religious norms
- Any other actions that result in **self-censorship**

Mapping Internet Censorship

Empirical data on what is censored & where

Open Net Initiative (ONI) did a study on Internet filtering covering 40 countries in:

1. Asia
2. Australia and New Zealand
3. Commonwealth of Independent States [Russia & former USSR states]
1. Europe
2. Latin America
3. Middle East and North Africa
4. Sub-Saharan Africa
5. Unites States and Canada

Filtered Content Categories

Political
Social
Conflict/Security
Internet tools

Filtering Levels

No evidence of filtering
Suspected filtering
Selective filtering
Substantial filtering
Pervasive filtering

Other factors:

Transparency, Consistency

Mapping Internet Censorship

Empirical data on what is censored & where

Method:

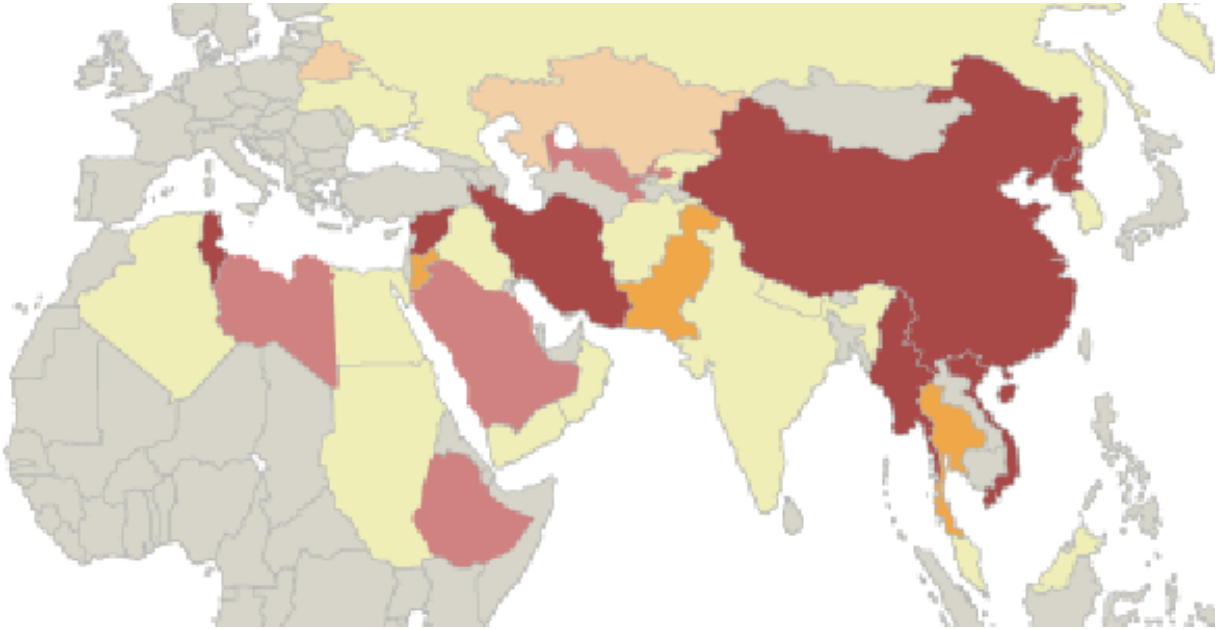
Special software was used by several researchers to automatically test if candidate websites in different categories were blocked.

Findings:

- **Asia** (mainly focused on **China**, but includes **Burma** & **Vietnam**):
  Practiced pervasive political and substantial social filtering.
- **Middle East and North Africa:**
  Practiced pervasive social and substantial political filtering.
- **Australia, New Zealand, Europe, Latin America , U.S.** & **Canada**:
  Limited filtering of social content (child pornography or abuse, racism, etc.).
- **Commonwealth of Independent States**:
  Varied, but most had limited filtering, except **Uzbekistan** with substantial political filtering.
- **Sub-Saharan Africa:**
  Had the lowest level of regulations, mostly due to lack of adequate infrastructure and resources.

Internet censorship on the national scale

The Internet is on the one hand being censored by governments in some countries, with censorship software imported from the West



- **More that 40 countries are filtering the Internet to varying degrees**
- **More than half a billion Internet users are being filtered worldwide** (32% of the world's Internet users!)

Source: ONI

Motives of the Censors

Why Censor?

Censors want to:

• "*protect the predominant ideology from which those benefit most who have attained power, wealth, status, and control within society*." and want to "*legitimize their eminence and the various social, political and economic arrangements they oversee.*"

White, H. (1997). Anatomy of censorship: Why the censors have it wrong. Lanham: University Press of America.

<u>Different states have different motives</u>

China:

The state censors to prevent content that could damage China's unity and sovereignty, harm ethnic solidarity, promote superstition, portray violence, pornography, gambling or terrorism, violate privacy, or damage China's culture or traditions or to prevent disseminating dissident and anti-government ideas and information to the Chinese public.

Saudi Arabia and several MENA countries:

The governments practice social filtering to protect '**public moral**' from offensive content such as pornography. But censorship of pornography may exist only as **part of the '*real reason*'** for blocking online content.

Motives of the Censors

States in the MENA region censor social content such as pornography, alcohol, homosexuality and similar material based on social and/or religious grounds.

Cuba:

State replaced the Internet with an intranet. It realizes that opposition movements may try to use the Internet to organize and communicate directly with the public, which may threaten the state's authority.

U.S.A. :

Congress passed the Communication Decency Act (CDA) in 1996 to reduce the chances of children accidentally encountering pornography on the Web. It was struck down by the constitution but the watered down version CDA II was later approved.

Accomplices from the West

Google, Yahoo! and other search engines censor results to maintain their business operations (MacKinnon, 2008). U.S.-based software companies (e.g., SmartFilter, Websense, etc.) are hired by authoritarian states to censor the Internet.

Circumventing Internet Censorship

Circumvention of Internet censorship is possible through **proxies**, which serve as a bridge between the client and the blocked online content.

A comprehensive study on some circumvention programs was done by the Global Internet Freedom Consortium in 2007. The study covered the following tools:

- **Freenet**: Best used for anonymous and censor-proof Peer-to-Peer connections
- **Triangle Boy**: Currently inactive, but was among the first generation solutions
- **Garden:** Active, but with a limited user base
- **Ultrasurf**: Used actively around the world for to circumvent web censorship
- **DynaWeb:** A set of tools to circumvent any type of Internet censorship
- **Tor:** Used mostly in the West for anonymity purposes

- There is a lack of studies on circumvention, including legal implications of developing or using such software although some technical guides on how to install and use some circumvention tools are available.

Anonymizing Connections

- Anonymizing a connection is some times the difference between life and death
- Available programs (e.g., Tor) not always working in times of crises
- Technology have dual use (can be used for good or bad purposes (e.g. hacking)
- Cyber activists do not have enough training on how to remain anonymous
- Surveillance is a very serious threat to anonymity
- Facebook and other social networks make anonymity harder
- Western companies (e.g., Twitter) can hand over information about users
- Realistically, total anonymity will be rejected by all countries (even democratic)

Companies accomplices?

- Censorship can be on the level of the service provider (Youtube, Blogger, etc.)
- Commonly used reasons for removal of data is intellectual copyright
- Violence, religious bigotry, racism, etc. are reasons to remove content
- Companies can use TOS rules to censor content without user approval
- Most global companies are based in the US and oblige to US laws
- Domains can be taken down through legal orders (e.g. http://megaupload.com)
- Wikileaks prevented from using credit companies, banks, hosting companies, etc.
- Facebook and other social networks make anonymity harder
- Western companies (e.g., Twitter) can hand over information about users
- Realistically, total anonymity will be rejected by all countries (even democratic)

Where Does Internet Governance Weigh in?

IG can have a role in two parallel paths:

1- Access to the Internet:

- Enhancing infrastructure, especially in developing countries
- Promoting education
- Raising Awareness & encouraging civil society participation
- Creating cheaper, better technology

2- Freedom of expression:

- Reforming international and national laws
- Promoting human rights online
- Enhancing security/privacy in software production
- Identifying violations against bloggers, etc. and penalizing violators
- Preventing abuse of Intellectual Property to limit freedom of expression
- Protecting consumers from privacy breaches & surveillance

Consequences & Implications

Internet censorship is a new subject and its implications are hard to measure.

But it can be argued that it has violated **human rights** in breaching **Article 19** of the Universal Declaration of Human Rights, which says:

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."*

An attempt was made to define some borders through the **Johannesburg Principles** , which state that a restriction on freedom of expression should be permitted only when "***the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest***".

The dilemma may be in defining what "***national security interests***" are!

Consequences & Implications

But does the public think that Internet censorship could have good effects?

- In China, **over 80%** of a PEW survey respondents agreed with Internet censorship.
- In the U.S.A., **47% of 4,247 respondents** agreed somewhat or strongly with Internet censorship of certain content.

Three reasons why some may support censorship:

1. Protect children from pornography.
2. Avoid material that could offend persons (privacy, safety) or the community.
3. Prevent content on issues that are illegal (terrorism, creating, planting bombs, etc.).

But the Internet is not controlled by a central entity. So to have Internet censorship regulated and not abused, it will have to be on an individual and **voluntary** basis.

UNESCO's drafted in 2007 a "***Code of Ethics for Information Society"*** that can be voluntarily applied by states and by the private sector.

Are states that already violate Article 19 of the Universal Declaration of Human Rights expected to voluntarily abide by such a code?

Questions

Thank you for your time

Follow us on www.diplomacy.edu