

Chapter 81

Internet Regulation and Online Censorship

Nikolaos Koumartzis

Aristotle University of Thessaloniki, Greece

Andreas Veglis

Aristotle University of Thessaloniki, Greece

ABSTRACT

This paper explores the development of Internet regulation policies worldwide since the birth of the World Wide Web, describes the advantages and disadvantages of the main filtering methods in use today, and presents two of the most important Internet Regulation Systems (IRS) implemented in authoritarian regimes and Western democracies around the globe. Moreover, the authors propose the conduction of well-designed surveys worldwide in order to measure Internet User's opinion and use such results as a starting point for developing a fair "Internet Regulation System" (fair IRS) in the future. Last, the authors introduce a new online tool for conducting related surveys, www.WebObserver.net project.

1. INTRODUCTION

There is a quite widespread (but false) impression today that Internet is the only media that, thanks to its nature, cannot be regulated. "The Internet interprets censorship as damage and routes around it" John Gilmore, co-founder of the Electronic Frontier Foundation, said in 1993 at the Time Magazine (Elmer-Dewitt 1993). Unfortunately, since then many things have changed in disfavour of freedom of speech on the web.

Over the last decade, Internet regulation is on the rise: in 2006 OpenNet Initiative stated that at least 26 countries were using content blocking systems (OpenNet Initiative 2008), in 2009 Reporters Without Borders stated that "some sixty countries experienced a form of Web censorship, which is twice as many as in 2008" (Reporters Without Borders 2010), while through 2010 the OpenNet Initiative became more specific by documenting Internet filtering policies by governments in over forty countries worldwide (Noman and York 2011).

DOI: 10.4018/978-1-5225-7113-1.ch081

At the epicentre of this Internet regulation worldwide battle is China: a country that has the world's largest Internet population (390 million Internet users in 2009 with penetration rate at 28.9 percent according to ONI 2011a) and at the same time, as OpenNet Initiative stated in 2011, "the world's most advanced Internet censorship and surveillance regime in cyberspace" (ONI 2011b).

Moreover, according to related surveys conducted on massive scale, Internet users are split in the half regarding where they stand for about Internet regulation (GlobalScan Incorporated 2010), while smaller surveys (focused on limited but highly educated samples) show that the majority of the Internet users prefer the implementation of some sort of "open" Internet regulation system (i.e. a system that they will be able to interact with, enriching or correcting its database) than no Internet regulation at all (Koumartzis and Veglis 2010 & Koumartzis 2008).

As stated by John Palfrey, executive director of the Berkman Center for Internet and Society at Harvard Law School, this issue is an open question, as "Some people would say that certain kinds of information should be banned" (Blau 2007). There is a worst case scenario though, as described by S. N. Hamade in which "filtering creeps into the system in an ad hoc way without formal evaluation of the standards [...]" (Hamade 2008).

In order to avoid this scenario, an IRS must be developed fair enough to be accepted by the majority of the Internet users. This has to be done via collaboration between those who regulate (i.e. governments) and those who are being regulated (i.e. Internet users, ISPs etc.), a collaboration that can be proven profitable for both sides (as stated in Li and Zhang 2009).

In a recent paper, the authors supported that even if the problem of Internet regulation is not of a technical nature, the solution can be found via a proper technical design and they went even further by proposing a blueprint for such a fair "Internet Regulation System" (fair IRS), able to handle specific kinds of illegal online content (Koumartzis and Veglis, 2012).

This chapter is organized as follow. The authors explore (in section 1) the development of Internet regulation policies since the birth of the World Wide Web, describe (in section 2) the main filtering methods in use the last decade and then proceed (in section 3) by presenting (and taking as a "guide") two current Internet filtering systems that are already implemented in national level around the world. Afterwards, they address (in section 4) the question "what the Internet users believe about the necessity of the Internet regulation systems?" by presenting results from past and new related surveys in different countries. Results from completed surveys in Germany and Russia and preliminary results from currently running surveys in India and Kosovo are being presented for the first time, thanks to the WebObserver.net International Project. Last, concluding remarks and future work is being discussed (in section 5), while an online tool for researchers is presented for conducting related surveys (www.WebObserver.net) worldwide with ease and efficiency.

2. ONLINE FILTERING POLICIES AROUND THE WORLD: A BRIEF HISTORY

When the World Wide Web was initially set up in 1990 (with the introduction of HTML), Internet users were able to access websites through a very simple and direct procedure as shown in Figure 1.

Until the end of 1994, there were already 3.2 millions hosts servers and 3.000 websites online that Internet users could access freely no matter from where they were connected (Fake 2008). Soon after, the freedom of Internet access was about to change in a different way from country to country; China

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/internet-regulation-and-online-censorship/213875

Related Content

The Role of Religiosity in Technology Acceptance: The Case of Privacy in Saudi Arabia

Rami Mohammed Baazeem (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications* (pp. 1787-1808).

www.irma-international.org/chapter/the-role-of-religiosity-in-technology-acceptance/213884

The World is Polluted With Leaked Cyber Data

Ivan D. Burke and Renier P. van Heerden (2019). *National Security: Breakthroughs in Research and Practice* (pp. 497-513).

www.irma-international.org/chapter/the-world-is-polluted-with-leaked-cyber-data/220897

Border Security and Cooperative Initiatives to Counter Illicit Drug Trafficking: The Case of Jamaica and the USA

Suzette A. Haughton (2017). *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 104-120).

www.irma-international.org/chapter/border-security-and-cooperative-initiatives-to-counter-illicit-drug-trafficking/164719

Who Watches?

(2022). *Modern Day Surveillance Ecosystem and Impacts on Privacy* (pp. 41-63).

www.irma-international.org/chapter/who-watches/287143

Biometric Spoofing and Anti-Spoofing

Zahid Akhtar (2017). *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention* (pp. 121-139).

www.irma-international.org/chapter/biometric-spoofing-and-anti-spoofing/164720