BURNING THE VILLAGE TO ROAST THE PIG[1]

Censorship of online media
A paper for the OSCE workshop
'Freedom of the Media and the Internet'.
30 November 2002

AUTHOR: Felipe Rodriquez
felipe@xs4all.nl

[1] "*Any content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig*." Judge Stewart Dalzell, ACLU -v- Reno, 11 June 1996

Censorship

In the strict sense, censorship is an act of government in which it becomes criminal to obtain or disseminate certain types of information. The term is also use to describe restrictions on the way *ideas are expressed, such as using profanity.*

The purpose of censorship is to control people by influencing the way they think and act. It is understood that people's thoughts and actions are shaped by the information they have available. To the extent one can control what information people have, one is able to control the people themselves. For this reason, censorship is very common among, perhaps even essential to, totalitarian governments.

Source: Wikipedia, the Free encyclopedia

Introduction

Since the arrival of the Internet as a popular medium to exchange information, concerns have been expressed about access to online content deemed to be offensive or dangerous.

The absence of national borders on the Internet has an effect on the availability and proliferation of controversial information. Community standards are a local affair, and different communities have different standards. Information that in one country is illegal, such as bestiality in the United States, is legal in another, such as the Netherlands. Vice versa neo nazi propaganda is constitutionally protected in the United States, whereas it is illegal in the Netherlands. In the analog age this was a trivial difference, as it was possible to control the distribution of the carrier of the information, such as paper, audio/video cassettes or electromagnetic waves. There was always a small amount of clandestine distribution but the public majority was mostly unable to access censored information.
Digital communications has changed the paradigm, and we now live in a world where information is not restricted by physical boundaries, except for a few exceptions such as China and Saudi Arabia. On the Internet a Dutch person can access any information on the US part of the Internet, even if that information is not legal in the Netherlands. And a US national can access any kind of information in the Netherlands that is illegal in the US.

Censorship laws are sometimes seen by politicians and governments as the solution to these problems, and several countries have implemented comprehensive systems of censorship on the Internet. Parents, schools and other entities have turned to privately manufactured Internet rating and filtering programs, with varying rates of success.

The debate about online content is still very much alive, and none of the available solutions to protect against offensive content are completely satisfactory. At one extreme of the debate are religious leaders and community groups that want some sort of protection against offensive content on the Internet in a desperate attempt to protect the local community standards. On the other extreme are civil liberty groups that see any form of censorship as a threat to freedom of speech. Regardless of the moral position on censorship, the reality is that effective censorship on the Internet is incredibly difficult without harming legal access to information.

This paper aims to provide a bird’s eye view of online censorship and the technologies that are used to implement or circumvent censorship; it is not an exhaustive analysis.

Overview of Internet technologies

The debate about censorship of online media is usually focussed on the World Wide Web[2] and Usenet newsgroups[3]. The Internet provides much more than just the Web, Email and the Usenet. In any discussion about censorship we need to define what technology we are talking about. I provide here a limited overview of available technologies, to aid us in the discussion about censorship of online media.

Email

"E-mail, or email, is short for "electronic mail" and refers to composing, sending, and receiving messages over electronic communication systems. Most e-mail systems today use the Internet, and e-mail is the most popular use of the Internet." [4] Email is not limited to private conversations; there are numerous public Email mailinglists on the Internet that anyone can subscribe to.

Many people that have used the Internet for a while receive unwanted email, also called Spam[5]. These emails are often scams or advertisements for erotic products, such as penis enlargement or live sex shows. Some of the Emails the author regularily gets in his mailbox have subject lines such as:

"Get Christmas Money – Santas Best Kept Secret"
"Make your love life better, grow inches now"
"One form, one time, thousands of instant cash prizes!"
"Your health care…"
"Add ¼ inch in one week"
"Sample viagra"
"Hello its teresa, naughty girls who love to smoke"
et cetera

In some countries the senders of commercial advertising emails need to include an opt-out mechanism, that enables the receiver to unsubscribe from that particular spam list, but in practice these opt-out mechanisms rarely work. The author has dealt with the spam problem by turning on a set of filters provided by his provider, XS4ALL. This strategy identifies 99% of spam, and has enabled the author to receive these messages in a separate folder.

The World Wide Web

The Web is usually the main target of Internet censorship proposals. The Web and Email are the most visible components of the Internet. Therefore the Web arouses much of the controversy about online content. A lot of content on the World Wide Web is static, but not all of it is. Examples are the many webcams[6] that are all but static, and provide a constantly changing picture of the environment the webcam is pointed at. Webcams are sometimes used by users to engage in amateur pornography, to share their pornographic fantasies with an audience[7].

[2] The Web, see glossary
[3] see glossary
[4] Source: www.wikipedia.org
[5] See glossary under Spamming
[6] see glossary
[7] see http://www.webcamnow.com - unmonitored adult area

Usenet

"*Usenet (also known as Netnews) is a set of protocols for generating, storing and retrieving news "articles" (which resemble mail messages) and for exchanging them amongst a readership which is potentially widely distributed. It is organized around newsgroups, with each newsgroup carrying articles about a specific topic.*"[8]

Close to a million messages are published in Usenet discussion groups every day[9], generating little over 130 gigabyte[10] of data. One gigabyte equals over 1,000 books of text[11]. Google provides a searchable archive of the Usenet[12]. A small percentage of the messages on Usenet contain pornographic content[13] or are used to exchange pirated software[14]. Commercial Spam messages are prolific on the Usenet, and concerned citizens have taken it upon themselves to censor these messages by erasing them for the rest of the community, a dubious activity because it takes away the choice of the individual to legally access the information and filter it if deemed necessary. These grassroots community censors defend themselves with the argument that without their activity the Usenet newsgroups would soon be flooded by endless amounts of commercial advertising.

IRC & Instant Messenger technology

"Internet Relay Chat (IRC) is a form of instant communication over the Internet. IRC is a predecessor to the class of applications known as instant messaging.
IRC has a decentralized network of servers that can be accessed by special client programs. The protocol for IRC is open, and there are many client (and server) implementations. Unlike popular instant messaging applications, there is not an inherent login id that one must acquire; it's typically a much more anonymous medium than instant messaging."[15]

"An instant messenger is a computer application which allows instant text communication through a network such as the Internet. An instant messenger is a client which hooks up to an instant messaging service. Instant messaging differs from email in that conversations over instant messaging mediums happen in real-time. Generally, both parties in the conversation see each line of text right after it is typed (line-by-line), thus making it more like a telephone conversation than exchanging letters."[16]

IRC enables private communications and group chats, group chats can be private and restricted, or open to the public. IRC and some of the instant messenger technology also enable the user to transmit files to other users, and with robot software this file distribution facility is sometimes automated. The content on IRC is highly dynamic, consisting of the private and public chat messages that users exchange, censoring or filtering IRC is unlikely to be successful because of these dynamics.

Many of the concerns about safeguarding children from predatory behaviour by adults on the Internet concern chat or messenger technology.

---

[8] Source http://www.wikipedia.org/wiki/Usenet
[9] Usenet Stats -http://news.gamma.ru/stats-week.html
[10] see glossary
[11] Computer Basics, Storage devices - http://dragon.ep.usm.edu/~it365/module/Basics/storage.htm
[12] Google groups at http://groups.google.com
[13] see alt.binaries.erotica.* Usenet groups
[14] see alt.binaries.warez.* Usenet groups
[15] Wikipedia - http://www.wikipedia.org/wiki/IRC
[16] Wikipedia - http://www.wikipedia.org/wiki/Instant_messaging

Streaming Media

Streaming media are the online alternative to traditional broadcasting. Streaming media client[17] software enables the user to access live or archived audio and video content. Many radio stations provide their broadcast online through streaming media technology, and some television broadcasters do as well. Streaming media technology is not limited to traditional broadcasting organizations; it can be used by end-users as well to participate in video chat groups or to broadcast their own productions. Some providers of pornographic content use streaming media technology for their pay-per-view products.

Peer to Peer technology

"Put simply, peer-to-peer computing is the sharing of computer resources and services by direct exchange between systems. These resources and services include the exchange of information, processing cycles, cache storage, and disk storage for files."[18]

Peer to peer technology acquired popularity and a certain amount of notoriety with the introduction of the Napster[19] file sharing service, which provided a very popular music swapping platform. The service soon became the object of scrutiny from the RIAA, the Recording industry Association of America, because much of the music that people exchanged through the Napster service infringed the copyright of the recording industry. The RIAA litigated against Napster, and was ultimately able to shut it down. Peer to peer file exchange technology is still around today, and is more popular than ever.

It is important to keep the dynamic nature of information on the Internet in mind, as this provides important challenges to any attempt to censor online content.

[17] see glossary
[18] What is Peer to Peer - http://www.peer-to-peerwg.org/whatis/
[19] see glossary

Censorship Today; a few examples

Historically the censor worked towards enforcing local community standards, this was possible because analog information was mostly locally distributed. Enforcement of censorship was relatively easy because information had a physical carrier, and a license was required when broadcasting through the ether. The use and distribution of these carriers could be controlled, the carrier could be destroyed or confiscated, or a licensed broadcaster could be threathened and closed down. Such controls have become unpractical since the popularization of the Internet.

Digital information can be infinitely replicated without cost inhibition; the absence of significant cost of reproduction has caused an explosion of published information. The global information infrastructure has transcended the region, as it is by definition a global grid. The effects of infinite duplication and internationalization of information pose an impossible challenge for the censor. The resources that are required to review and block the more than 4 billion pages of web content around the world are mind boggling.

One important thought to keep in mind is which technology we talk about when we are discussing online censorship. Are we talking about the World Wide Web, or about Email, or about chatboxes, or about peer to peer file exchange networks, or about streaming media, or about Usenet Newsgroups? Discussions about online censorship are usually limited to the Web, but the Internet offers so much more than just the Web.

Government Censorship

How does one enforce local community standards in a global environment?

China has implemented the most comprehensive censorship system on the Internet.. The Internet is somewhat of a paradox to the Chinese authorities, as it provides access to information that will be crucial to the countries industrial and scientific development. Yet at the same time the Internet greatly complicates the pursuit of internal security, and officials have warned that the Internet could be "*harmful to social stability*"[20]

The system of censorship China has implemented involves routers that block access to certain IP addresses[21], surveillance of users, the use of informers, arrests and seizures. [22] China focusses primarily on websites and Email.

Technologically the system is quite crude, because thousands of websites may be grouped under a single IP-address. Blocking the IP-address blocks all those websites, even if the content on those sites is not controversial. Implementing an IP-blocklist also degrades network performance; large blocklists can cause serious performance problems. *"Blocking can be done only intermittently, because the software does not have enough computer power to block every objectionable site all the time"*[23] An IP-blocklist can be defeated by changing, or rotating, the IP-address of a website. Recently the Ministry for Public Security implemented a system of domain name hijacking, which is a somewhat more sophisticated system of access control. The technique works by falsifying the records in Domain Name Servers[24] (DNS) throughout China. The domain name system is the connection between a domain name, such as www.xs4all.nl, and the IP-address of that

[20] Zhao Ying, "information and security issues," Jingji Guanli, no.5, may 5. 1998pp as printed in Rand Report 'You've got dissent!' pp48 chapter two, government counter strategies
[21] see glossary
[22] Rand Report 'You have got dissent!' pp49 chapter two
[23] Rand Report 'You have got dissent!' pp64 chapter two
[24] see glossary

site. By interfering with the DNS system the Chinese authorities are able to divert traffic[25] to certain domains to unrelated IP-addresses, thereby blocking access to the website and diverting traffic to another (government controlled) website. [26] There are some indications that China has developed the capability to automatically block individual web pages by using content rules, based on individual words, or combinations of words that appear on the page.[27]

It is estimated that the government employs as many as 30.000 people to enforce Internet censorship.[28] *"..Chinese filtering is quite effective, not as granular as Saudi Arabia," [29]*

Saudi Arabia has a similar, but less effective, system of censorship, aiming to censor offensive and unislamic content.[30] It is estimated that Saudi Arabia blocks around 400.000 IP addresses. [31] In Saudi Arabia a user that tries to access a censored website is showed a notice that the site has been blocked, this is not the case in China.[32]

Saudi Arabia and China are two examples where censorship on the Internet has been implemented somewhat successfully. It is noteworthy that both are repressive regimes, which has enabled these states to take control of the distribution of digital content, the use of informers and intimidation. Other countries, such as Singapore, South Korea, Iran, Syria etc have implemented similar censorship systems, with varying rates of success.

Although these censorship frameworks have achieved a degree of success in supressing information, it must also be noted that a lot of legal and uncontroversial content is filtered as a consequence, because the technological tools that are implemented are crude and usually affect entire websites or even hundreds of webservers that share the same IP-address. Important elements of the censorship framework in all these countries are the low-tech solutions, such as the use of informers, arrests, seizures and intimidation.

Implementing online censorship in a democratic nation is infinitely more complicated, and so far there have been very few successful attempts at doing so.

Australia has the most comprehensive system of censorship among democratic nations since it implemented the "Broadcasting Services Amendment (Online Services) Bill 1999".

> *"The Broadcasting Services Amendment (Online Services) Act 1999 commenced operation on 1 January 2000. To date (November 2002) it has been implemented in a way that does not require ISPs to block access to content on overseas sites. (The government regulator has the power to require ISP blocking if they consider the current implementation of the law to be inadequate).*
>
> *However, ISPs/content hosts are required by law to delete Australian-hosted content on receipt of a take-down notice from the government regulator, i.e. the Australian Broadcasting Authority ("ABA").*

[25] see glossary
[26] Forbidden sites hijacked all over China, http://www.dit-inc.us/report/hj.htm - press release from Dynamic Internet Technology
[27] Online Journalism review – The shrinking frontier - http://www.ojr.org/ojr/world_reports/1037922526.php
[28] http://www.chinaonline.com/commentary_analysis/thiswk_comm/020320/C02031231.asp - China Online - 'A glimpse of China's Business, technology revolution 20 march 2002
[29] Quote by harvard researcher Ben Edelman, Online Journalism review – The shrinking frontier - http://www.ojr.org/ojr/world_reports/1037922526.php
[30] Documentation of Internet filtering in Saudi Arabia – http://cyber.law.harvard.edu/filtering/saudiarabia
[31] Human Rights Watch Report Saudi Arabia – http://www.hrw.org/wr2k2/mena7.html
[32] Online Journalism review – The shrinking frontier - http://www.ojr.org/ojr/world_reports/1037922526.php

The regime is complaints based. The ABA implemented a Complaints System which enables Australian citizens to lodge complaints about Internet content that is, or is likely to be, classified/rated:

- *R18 (information deemed likely to be disturbing or harmful to persons under 18 years),*
- *X18 (non violent sexually explicit material involving consenting adults) or*
- *RC (Refused Classification/banned)*

by the Government censorship office, i.e. the Office of Film and Literature Classification ("OFLC"). Internet content (including text, static images and moving images) is classified using criteria set out in the Classification Guidelines for Films and Videotapes (not the Guidelines for Publications) established under the Commonwealth Classification Act.

- ***Content hosted in Australia**: The ABA issues take-down notices to ISPs and other Internet Content Hosts requiring them (under threat of fines) to delete content on their servers (e.g. Web, Usenet and FTP) that is classified X18 or RC, and also R18 if access to R18-rated material is not subject to an ABA approved adult verification system (AVS). The approved AVS for R18 material requires sites, including non-commercial sites and those who charge no fee for access, to collect personal information from visitors to their site, such as credit card details or a copy of a driver's licence or birth certificate, before granting them access to R-rated information. The ABA is required to have Australian-hosted content classified by the OFLC before issuing a final take-down notice (an interim take-down notice is issued in the case of material likely to be classified X18 or RC, but not R18).*
- ***Content hosted outside Australia**: The ABA issues notices to approved filtering/blocking software providers informing them to add content the ABA considers likely to be classified X18 or RC (but not R18) to their blacklist. Australians are not required by law to use filtering/blocking software products. The ABA is not required to have content on overseas sites classified by the OFLC, the ABA makes its own determination of whether the content would be likely to be classified X18 or RC. "*[33]

The problem with Australian Internet censorship is obvious; it only applies to local content, as Australia has no jurisdiction or technology to apply censorship to information that is hosted outside the country. The government promotes the use of commercial filtering software for this purpose. Implementing the Chinese technology framework is too crude for Australia, as this would interfere with the freedom of its citizens to access content that is legal and uncontroversial.

The Australian censorship legislation has symbolic value; the government can say that it has implemented limitations on the use of the Internet with the aim to protect community standards. There is no measurable effect on the availability of harmful content overseas when the user chooses not to use commercial filtering software. The legislation is an effort in managing perceptions; there seems to be a perception in some parts of the Australian community (especially among church leaders) that the Internet is an unsafe environment, to counter this notion the government implemented legislation to create the new perception that something is being done by the government about offensive content. The Australian censorship framework is a product of domestic politics, and has little to do with result driven policy.

Indications are that locally censored information has been moved overseas, as it is trivial to relocate a website to another jurisdiction.[34] Australia's censorship focuses primarily on websites and newsgroups.

[33] http://www.efa.org.au/Issues/Censor/cens1.html - Electronic Frontiers Australia publication "Internet Censorship in Australia"

[34] http://www.efa.org.au/Issues/Censor/cens1.html - Electronic Frontiers Australia publication "Internet Censorship in Australia"

Commercial Censorware

Censorware[35] is *"software which is designed to prevent another person from sending or receiving information (usually on the web)."*[36] It is commercial filtering software that can be purchased by users, it allows the user to install filters that limit access to certain information on the Internet. In Australia ISP's[37] must make filtering software available to their customers at cost price. Examples of such software are WebSENSE, Net Nanny, CYBERsitter and Cyber Patrol.

Censorware is a popular alternative to government censorship, because it allows the user to choose if filtering is applied. It provides parents with a tangible tool to protect their children from offensive content.

Despite this promise, there are considerable problems with commercial filtering software. Overblocking or underblocking are a concern, because access to harmless information is often denied, or access is inadvertedly granted to offensive content. [38]

A sample [39] of the mistakes that can be found in censorware:

- *BESS blocked the home pages of the Traditional Values Coalition and Massachusetts Congressman Edward Markey.*
- *Cyber Patrol blocked MIT's League for Programming Freedom, part of the City of Hiroshima Web site, Georgia O'Keeffe and Vincent Van Gogh sites, and the monogamy-advocating Society for the Promotion of Unconditional Relationships.*
- *CYBERsitter blocked virtually all gay and lesbian sites and, after detecting the phrase "least 21," blocked a news item on the Amnesty International Web site (the offending sentence read, "Reports of shootings in Irian Jaya bring to at least 21 the number of people in Indonesia and East Timor killed or wounded").*
- *I-Gear blocked an essay on "Indecency on the Internet: Lessons from the Art World," the United Nations report "HIV/AIDS: The Global Epidemic," and the home pages of four photography galleries.*
- *Net Nanny, SurfWatch, Cybersitter, and BESS, among other products, blocked House Majority Leader Richard "Dick" Armey's official Web site upon detecting the word "dick."*
- *SafeSurf blocked the home pages of the Wisconsin Civil Liberties Union and the National Coalition Against Censorship.*
- *SmartFilter blocked the Declaration of Independence, Shakespeare's complete plays, Moby Dick, and Marijuana: Facts for Teens, a brochure published by the National Institute on Drug Abuse (a division of the National Institutes of Health).*
- *SurfWatch blocked such human-rights sites as the Commissioner of the Council of the Baltic Sea States and Algeria Watch, as well as the University of Kansas's Archie R. Dykes Medical Library (upon detecting the word "dykes").*
- *WebSENSE blocked the Jewish Teens page and the Canine Molecular Genetics Project at Michigan State University.*
- *X-Stop blocked the National Journal of Sexual Orientation Law, Carnegie Mellon University's Banned Books page, "Let's Have an Affair" catering company, and, through its "foul word" function, searches for Bastard Out of Carolina and "The Owl and the Pussy Cat."*

[35] see glossary
[36] http://censorware.net/article.pl?sid=01/02/10/2241204
[37] see glossary
[38] Internet Filters, A public policy report, Marjorie Heins & Christina Cho, Fall 2001 – National Coalition Against Censorship - http://www.ncac.org/issues/internetfilters.html
[39] Internet Filters, A public policy report, Marjorie Heins & Christina Cho, Fall 2001 – National Coalition Against Censorship - http://www.ncac.org/issues/internetfilters.html

The PICS/ICRA illusion – Filtering and rating

Attaching labels to content on the Internet is often promoted as a way to protect children from harmful content, while at the same time not preventing adult access to that information. One of the ways that has been promoted to create a child friendly Internet was the PICS initiative, the Platform for internet Content Selection."*The PICS specification enables labels (metadata) to be associated with Internet content. It was originally designed to help parents and teachers control what children access on the Internet, but it also facilitates other uses for labels, including code signing and privacy*."[40]

Content labelling mechanisms have often been promoted as the best compromise in censorship, as they provide a selective filtering mechanism where the user or parent can choose what type of information is filtered. It remains a popular alternative to censorship in government circles and with industry lobbyists. But it is unrealistic to have any expectations about labelling technology, the debate has been going on for more than 7[41] years and very little progress has been made. Discussions about content labelling are mostly theoretic, and the words 'if adopted' are often repeated.

Content labelling is unlikely to succeed because it suffers from the chicken and egg problem. As long as it is not widely used, users have no incentive to label the content on their website. And content labelling will never be widely used if insufficient users have labelled the content on their site. A user that today turns on label based content filtering in their browser effectively blocks access to most of the Internet, not exactly a display of a user-friendly technology that is likely to be adopted spontaneously by large amounts of people. In the absence of consensus with partners outside the EU implementation of a comprehensive content labelling system is unrealistic.

An additional problem with any content labelling system is the integrity of the label that the user attaches to his site. If someone had the intention to sabotage and pervert the content labelling system, he could mislabel offensive content as being suitable for all ages, with obvious effects.

There are quite a few concerns about content labelling in the civil liberties community. These concerns revolve around the fact that once information is labelled, it becomes very easy for a government to setup national systems of censorship based on these labels. Part of this concern is "*that governments would enforce or coerce the use of PICS facilitated systems. The probability of mandatory self-rating and prosecution for inadvertently mis-labelling, or failing to label, became obvious*."[42]

Content rating and filtering is one of three pillars in the EU Safer Internet Action Plan, and 8 million euro has been allocated to projects that study rating or facilitate and create rating and filtering technology. [43]

Child Pornography

In every debate about censorship child pornography is put forward as an argument in defence of online censorship. Child pornography and predatory behaviour are problems

[40] W3C Platform for internet Content Selection - http://www.w3.org/PICS/
[41] Chronology: PICS development and Internet censorship proposals - http://www.libertus.net/liberty/picsrisk2.html#1995
[42] The Net Labelling Delusion, saviour or devil - http://libertus.net/liberty/label.html
[43] Information Society – Safer Internet Action Plan - http://europa.eu.int/information_society/programmes/iap/index_en.htm

on the Internet, and can be encountered in obscure places. But it is not realistic to think that censorship is a solution. The illegal nature of the content causes it to be distributed underground, in chatrooms and transient newsgroups. The content and offenders are difficult to trace, and the communities that distribute it are not easily accessible to the general public.

Child pornography is a law enforcement problem. There is no country in the world where the distribution of this type of content is legal; it is the only content where a degree of global consensus has been reached. Law enforcement agencies routinely investigate online child pornography, and are having a good rate of success. Agencies are cooperating internationally to combat the problem. Law enforcement agencies have become proactive in recent years and undercover sting operations are used, such as the FBI's Innocent Images Task Force.[44]

Some Internet service providers have blocked access to certain newsgroups that are routinely used to exchange images containing child pornography.

Hotline systems

In June 1996 a hotline was established in the Netherlands to combat child pornography online. [45] This hotline provides a facility for Internet users to report child pornographic content on the Internet. The hotline has a permanent liason with the Dutch criminal investigation unit, and reports are forwarded to this unit. The hotline was a direct response to community concerns about child pornography on the Internet, and the fact that law enforcement agencies were unprepared to address this problem.

Hotlines have since been established in Australia, Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Ireland, Spain, Sweden, the UK and the U.S.A. [46]

The modus operandi of these hotlines varies, some hotlines will issue take-down notices, some will report illegal content to the police, some do both.

Hotlines provide an intermediate facility to report illegal content, as many law enforcement agencies do not yet provide quick and efficient mechanisms to report a complaint. One would expect government and law enforcement agencies to eventually take over the functions that hotlines are currently providing, because one usually reports a crime directly to a government agency, and not to a third party NGO[47]. Experts in the civil liberty community have expressed concern about the lack of due process in the procedures of hotlines.

Hotline systems are one of three pillars in the EU Safer Internet Action Plan, and 1.975 million euro has been invested by the European Commission in hotline projects. [48]

---

[44] The oregonian, "FBI fights child pornography online" 11/20/02, http://www.oregonlive.com/news/oregonian/index.ssf?/xml/story.ssf/html_standard.xsl?/base/news/1037797091130520.xml

[45] http://www.meldpunt.org/

[46] The association of internet hotline providers in Europe, list of members, http://www.inhope.org/english/about/members.htm

[47] see glossary

[48] EU information society – Safer Internet Action Plan - http://europa.eu.int/information_society/programmes/iap/index_en.htm

Commercial censorship – Intellectual property and copyrights

Peer-to-peer

Software-piracy[49] has existed since the beginning of software. It has always been possible to find illegal copies of virtually any software product online. Illegal software is distributed through a variety of technologies, the World Wide Web, the usenet newsgroups[50], The File Transfer Protocol[51], and more recently through peer-to-peer technology.
Software companies have learned to live with the fact that any copyright protection mechanisms will be broken, however sophisticated they may be. There are software patches[52] and tools available to break the copyright protection mechanisms of almost any available software product. It is a matter of pride for pirates to publish new software or software cracking tools[53] before, or just after, the product arrives in the shops.

It is only in recent years that content such as music and screen content has become digitized. Digitized content has very similar attributes to software, such as ease of online distribution and problems with copyright protection mechanisms that are routinely broken. Technologies such as Napster[54] and other peer-to-peer protocols, together with the arrival of broadband technologies in the home, provide a convenient and enormously popular method for the sharing of software, music and screen content among users.

The music industry counter attacked by pursuing Napster and other companies such as Morpheus[55] and Kazaa[56] in the courts. Napster closed down, but peer-to-peer file sharing technologies fragmented into a dozen different networks and are more popular than ever. Most of these networks have no central point of control such as Napster had, making it impossible to litigate against a single entity to close down these networks.

"On July 25, 2002, Representative Howard Berman (D-Cal.) introduced a bill, H.R. 5211 in the House of Representatives that would give copyright owners the right to violate the law in their efforts to stop the unauthorized circulation of their works on peer-to-peer networks." [57] [58] If passed this bill would allow copyright holders to organize sabotage against copyright infringement, a form of state sanctioned cyber terrorism. The bill has not yet passed, and has been referred to the US Subcommittee on Courts, the Internet, and Intellectual Property. [59]

A recent research paper published by computer scientists working for Microsoft Corporation concluded that attempts to stop the swapping of copyrighted works on online peer to peer networks will not work. [60]

---

[49] see glossary
[50] see glossary
[51] see glossary
[52] see glossary
[53] see glossary
[54] see glossary
[55] see glossary
[56] see glossary
[57] The Berman P2P Bill: Vigilantism Unbound - http://www.eff.org/IP/P2P/20020802_eff_berman_p2p_bill.html
[58] a copy of the bill can be found at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h5211ih.txt.pdf
[59] Bill Summary & Status for the 107th Congress - H.R.5211 status - http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR05211:@@@X
[60] BBC news - http://news.bbc.co.uk/2/hi/technology/2502399.stm
The Darknet and the future of content distribution - http://crypto.stanford.edu/DRM2002/darknet5.doc

Denial of Service Attacks[61]

A denial of service attack is a form of censorship, because it disables access to information through sabotage and flooding.

Although H.R.5211, if passed, will allow copyright holders the right to attack piracy, such attacks are already happening to some degree. On peer-to-peer networks one is likely to find many spoof files. Certain newsgroups, where pirated software is exchanged, are regularily bombed with thousands of empty messages.[62]

The best documented denial of service attacks against content on the Internet were organized by members of the Church of Scientology (CoS)[63]. CoS members or symphatizers have tried to permanently erase the newsgroup alt.religion.scientology by issuing forged control messages that removes the group from Usenet newsservers around the world. When that failed, they bombed the newsgroup with thousands of duplicated messages, in order to silence the discussion among critics of the church. Individual messages from critics were also routinely cancelled (erased).

Search engine censorship

Search engines have become an important access tool to the Internet. It is the tool of choice for people to locate information, and for some people it has taken the place or the Universal Resource Locator (URL)[64] method of typing the entire address of a website.

CoS is a litigious organization, and lawyers are often used to intimidate critics and other organizations in order to prevent dissemination of copyrighted or critical materials. In May 2002 the church *"threatened to sue Google[65] for contributory copyright violations for merely listing links to Web pages that, the Scientologists said, illegally published copyrighted passages. The church demanded that Google remove the links to the site, Operation Clambake[66], from its automated search results*."[67] The request resulted in the removal of an entire website, xenu.net, from the Google search archive. CoS typically requests removal of all content on a site, alleging "*wholesale, verbatim copyright infringement*".[68] Once Google became aware of the discrepancy between the alleged copyrighted works, and the actual copyrighted works, it quickly restored access to most of the blocked website.

Harvard Law School researchers found at least 100 sites missing from search results when accessing Google sites meant for French and German users.[69] Google does not include certain web sites in the French and German versions of its search engines, in particular neo-Nazi or white supremacy sites that have content that might be deemed illegal to publish in France and Germany.
China in late August blocked access to the Google and altavista Internet search engines for a brief period[70]; diverting users to local Chinese search engines instead.

---

[61] see glossary
[62] see alt.2600.warez newsgroup
[63] see glossary
[64] see glossary
[65] see glossary
[66] see glossary
[67] San Jose mercury editorial, "Scientology, Google and the First Amendment", May 02 2002, http://www.siliconvalley.com/mld/siliconvalley/business/columnists/3185788.htm
[68] Wired News, "Google Restores Church Links" Mar 22 2002, http://www.wired.com/news/ebiz/0,1272,51257,00.html
[69] Harvard Law School – "Localized Google search result exclusions" - http://cyber.law.harvard.edu/filtering/google/
[70] Online Journalism Review – The shringking frontiers - http://www.ojr.org/ojr/world_reports/1037922526.php

Actions against online censorship – routing around censorship

Online censorship is a technological battle. Online censorship becomes more sophisticated every day, but so do the tools that circumvent filtering.

Mirroring[71]

Mirroring of information is the oldest form of anti-censorship technology. When a website gets censored, people usually mobilize to copy the content of that site to dozens of other websites around the world. There are many examples of such mirroring in the short history of censorship on the Internet. Mirroring is an extremely effective technique against censorship, and also very easy to apply. The censor would have to block all the mirrors of a site to completely prevent access to the controversial information.

IP rotation

In 1995 the entire XS4ALL website, hosting thousands of users, was blocked by German Internet providers in an attempt to block access to a radical magazine on that site. The block consisted of a refusal by German ISP's to route to the IP address of the XS4ALL website. As a countermeasure XS4ALL employed an IP-rotation mechanism that changed the IP-address of the website every couple of minutes. [72]

Triangle boy

Safeweb, a company that received funding from In-Q-Tel, the CIA's venture fund[73], released software called "Triangle Boy". The software is a peer-to-peer application that volunteers download onto their PCs. A user that has been denied access to any website by a censor can use the Triangle Boy software to circumvent the censorship. [74] Currently the Triangle Boy software only provides access to the Voice of America, because this service is blocked by the Chinese government.

Peekabooty

"*The goal of the Peekabooty Project is to create a product that can bypass the nation-wide censorship of the World Wide Web practiced by many countries.*"[75]

"*Peekabooty uses a complicated communications system to allow users to share information while revealing little about their identity. When a node receives a request for a web page it randomly decides whether to pass this on or access the page itself. It also only knows the address of its nearest partner. This makes it difficult to determine who requested what information and is designed to protect users from anyone trying to infiltrate the system from inside.*"[76]

---

[71] see glossary
[72] Message from Felipe Rodriquez to Michael Schneider about censorship counter measures - http://www.xs4all.nl/~felipe/WWW.old/press/schneider.html
[73] Safeweb Website - http://www.safeweb.com/investors.html
[74] Safeweb Website - http://www.safeweb.com/tboy_service.html
[75] About the Peekabooty Project - http://www.peek-a-booty.org/pbhtml/modules.php?name=Content&pa=showpage&pid=1
76 New Scientist, 19 feb 02, "Peekabooty aims to banish internet censorship" http://www.newscientist.com/news/news.jsp?id=ns99991948

Peacefire.exe

"Peacefire.org was created in August 1996 to represent the interests of people under 18 in the debate over freedom of speech on the Internet."[77]

Peacefire created a windows program, peacefire.exe that disables any popular Windows filtering censorware such as SurfWatch, Cyber Patrol, CYBERsitter, Net Nanny, X-Stop, PureSight and Cyber Snoop.

Internet Freedom Act

On the 2nd of October 2002 US House Policy Chairman Christopher Cox and US House International Relations Committee Ranking Member Tom Lantos introduced legislation to counter Internet jamming and blocking around the world.[78]

When passed *"the United States will develop and implement a comprehensive global strategy to combat state-sponsored and state-directed Internet jamming.The Office of Global Internet Freedom, established within the International Broadcasting Bureau, will tap both private sector and government resources to help Internet users to avoid government censors and state persecution."*[79] The bill will, if passed, provide $50 million USD to help software companies develop anti-censorship software.[80]

Camera Shy

"Camera/Shy is the only steganographic[81] *tool that automatically scans for and delivers decrypted content straight from the Web. It is a stand-alone, Internet Explorer-based browser that leaves no trace on the user's system and has enhanced security."*[82]

Camera Shy is an application that enables stealth communications, such software can be useful in countries where Email communications are regularily monitored and censored, such as happens in China.

Proxy Relays

One of the easiest ways to circumvent censorship is to use a relaying proxy server. Proxy servers are a technology that was invented to speed up web traffic. It is an intermediate server cache between the user and the webserver, and popular content is cached on these servers. By configuring a webbrowser to use a relaying proxy server, government censorship systems can be bypassed. [83]

Akamai[84] can be used to bypass Internet censorship, and a description of how this can be done was written by Bennet Haselton.[85] Many large corporations use Akamai to optimize their Internet traffic distribution, the websites of these companies can be accessed by creating a special URL that uses Akamai as a relay server. This technique is in essence the same as using a proxy relay server for circumvention.

---

[77] About Peacefire - http://www.peacefire.org/info/about-peacefire.shtml
[78] Bipartisan, Bicameral Bill Stops Internet Jamming - http://policy.house.gov/html/news_release.cfm?id=111
[79] Bipartisan, Bicameral Bill Stops Internet Jamming - http://policy.house.gov/html/news_release.cfm?id=111
[80] Wired News – China's cyberwall nearly complete - http://www.wired.com/news/politics/0,1283,56195,00.html
[81] see glossary
[82] Project camera Shy, summary, http://sourceforge.net/projects/camerashy/
[83] relaying proxy servers - http://www.cexx.org/anticens.htm
[84] see www.akamai.com
[85] Using Akamai to bypass Internet censorship, by bennett haselton, http://www.peacefire.org/bypass/Proxy/akamai.html

He halted and, with bewildered and horrified eyes, stared round him at the khaki mob, in the midst of which, overtopping it by a full head, he stood. "How many goodly creatures are there here!" The singing words mocked him derisively. "How beauteous mankind is! O brave new world …"
Aldous Huxley – Brave new World

Conclusions

The Internet is a reflection of the global society that we live in. The anarchist cookbooks are there, and so are the holocaust revisionists and consumers of bestiality. The availability of such content is a consequence of living in a global information and communications environment. In a global environment effective online censorship can only be implemented in strongly repressive environments or in situations where there is some form of global consensus and cooperation.

Implementing any kind of online censorship is a technological battle, any censorship technology can, and will, be defeated. To get a feeling for the inventiveness of people in defeating technological restrictions one only has to look at the history of software piracy, where companies have employed increasingly sophisticated protection mechanisms, only to see them cracked within days by skilled hackers. Implementing censorship has become a technological battle that cannot be won, except in extremely repressive regimes.

China has the most comprehensive censorship system and is having a degree of success with their implementation; this is being achieved by employing 30.000 people and using a mix of technological and repressive instruments. It is not assured that China will be able to keep up this censorship framework in the next decade. Savvy Internet users in China are not affected by the censorship; they can use technological tools and solutions to circumvent it, although there is always the risk of informers or active government surveillance of their activities

For a democratic nation there are no simple solutions. No democratic nation has come close to sanitizing the Internet in order to uphold the local community standards. The debate about content labeling remains just that; a debate. Despite EU investments and studies into content labeling technologies, there are no indications that the technology will provide us with a holy grail of online filtering; it is more likely that the online community will ignore labelling technology, because there are no incentives to start using it.

Sometimes the job of the politician consists of managing the perceptions of the electorate. From that point of view it is perhaps understandable that so many proposals have been made to sanitize the Internet. But implementation is another thing altogether, and most plans that aim to clean up the smut on the Internet are either technically unfeasible or they require a form of global consensus among users and publishers of content or they require enormous resources. Despite years of debate about filtering offensive content on the Internet no actions have actually led to a changed environment in any of the democratic nations. Odds are that this will remain so in the coming decade.

If there is consumer demand for filtering, for example to protect minors, then companies will jump at this opportunity to provide products and services that meet the demand. Products are already available, and although none of them are perfect, at least having these products gives the consumer the autonomy of making the decision to censor himselfe and his family. In any government sanctioned censorship framework that choice is taken away, with the likely side effect of censoring legal and uncontroversial content.

Glossary

(Source Wikipedia, the Free encyclopedia, www.wikipedia.org)

Cache - A cache in computer science is a short-term memory in a computer with quick access. A cache is intended to speed up access to a set of data. The cache will be a piece of memory that is faster (hence more expensive, hence smaller) than the principal data storage area for the data in question. The cache operates by storing a part of the data, allowing that part to be accessed more quickly. A speed-up is achieved if many accesses to the data can access the data in the cache. The reason caches work at all is that many access patterns in typical computer applications have locality of reference. There are several sorts of locality, but we mainly mean that often the same data is accessed frequently or with accesses that are close together in time, or that data near to each other are accessed close together in time.

Censorware - Censorware is a term used to describe content filtering software by its opponents. They point out that content filtering software acts as a effective restraint on speech, and that government-driven mandatory installation of content filtering software is equivalent to censorship. Censorware is often proposed as a solution to the problem of hate speech on the Internet. Opponents of censorware point out that these tools not only block other content in addition to hate speech, either unintentionally, or as part of the political agenda of the manufacturers of the content filtering software, but also fail to block all the hate speech.

Client - A Client is a system that accesses a (remote) service on another computer by some kind of network.

Congestion - In telecommunication, the term congestion has the following meanings:
1. In a communications switch, a state or condition that occurs when more subscribers attempt simultaneously to access the switch than it is able to handle, even if unsaturated.
2. In a saturated communications system, the condition that occurs when an additional demand for service occurs.

Denial of service attack - A denial of service (DoS) attack is a term used to describe certain forms of malicious damage to computer systems. The aim of such an attack is to prevent legitimate users from accessing their services. A DoS attacks is generated in a number of ways. There are three basic areas of attack - the consumption of limited resources, such as bandwidth, disk space or CPU time; alterations to configuration information, such as routing information or registry entries; and the physical disruption of networking components. The attack on resources has become increasingly popular, mainly through attempts to "flood" a network with excess or spurious packet data over the internet, thereby preventing legitimate traffic. Distributed denial-of-service (DDoS), where many computers work in unison to attack a target system, has also gained notoriety due to the efficient tools which are available to create and launch such an attack.

DNS - the Domain Name System, is a distributed database that handles the mapping between host and "domain names" which are more convenient for humans, and the numerical Internet addresses. That is, it acts much like a phone book, so you can "call" www.wikipedia.com instead of 64.78.205.6.

FTP - The File Transfer Protocol, (FTP) is a protocol that is to be able to transfer files between machines with widely different operating systems.

Gigabyte - A gigabyte is a unit of measurement in computers of approximately one thousand million bytes, (the same as one billion bytes in the American usage) or roughly 1000 megabytes.

Google - Google is an Internet search engine founded in 1998 by Larry Page and Sergey Brin, two Stanford Ph.D. candidates, who developed a technologically advanced method for finding information on the Internet. As of 2002, it was the most popular search engine.

Internet - As a proper noun, the Internet is the publically available world-wide, interconnected system of computers (plus the information and services they provide and their users) that uses the TCP/IP suite of protocols. Thus, the largest internet in the world is called simply "the" Internet.

IP address - The Internet protocol (IP) knows each host by a number, the so called IP address. On any given network, this number must be unique among all the hosts that communicate through this network.

ISP - Internet Service Provider (ISP), provider of Internet services. Most telecommunications operators are ISPs. Provides services like internet transit, domain name registration and hosting, dial-up access, leased line access and colocation.

Kazaa - KaZaA Media Desktop is a peer-to-peer file sharing application on the Music City network, developed by FastTrack for Consumer Empowerment. It is very similar to Morpheus, which also used the FastTrack protocol. Many consider KaZaA to be superior to other programs because of its file selection and fast transfer speeds. Countering that is KaZaA's use of spyware and adware installed as default with the main product. The Altnet software, also installed by default, is another problem, it allocates users' bandwidth to serve advertisements to others.

Mirror - On the Internet, a mirror is an exact copy of data stored in a different location. Popular sites use mirrors to reduce network traffic on any one server.

Morpheus - Morpheus is also the name of a file sharing client operated by the company Streamcast (formerly called Musiccity) that originally used the OpenNAP peer-to-peer platform. It has a web-based search interface, just like Audiogalaxy, though Morpheus searches all kinds of media, not just mp3. In 2001, Morpheus changed protocol from OpenNAP to FastTrack. On February 26th 2002, all Morpheus clients suddenly stopped working when the FastTrack protocol was updated and Morpheus users no longer were allowed to log into the network. This was apparently because of licensing disputes bewteen StreamCast and the owners of FastTrack. On March 2nd, a new Morpheus client using Gnutella as its P2P medium was released.

Napster - Created by Shawn Fanning, Napster was a music and file sharing service that made a major impact on the Internet scene during the year 2000. Its technology allowed music fans to easily share MP3 format song files with each other, thus leading to massive copyright violations.

Newsgroup - A newsgroup is a repository within the Usenet system for messages posted from many users at different locations. Newsgroups are arranged into hierarchies, theoretically making it simpler to find related groups.

NGO - A Non-Governmental Organization (NGO) is an organization which is privately funded (mostly by donations from the general public) and is independent from the government and its policies. Most often it is a non-profit organization.

NNTP - NNTP - Network News Transport Protocol. A TCP-IP protocol based upon text strings sent over 7 bit ASCII TCP channels. It is used to transfer articles between servers as well as to read and post articles. Defined in RFC 977. The format of messages is specified by RFC 1036.

Operation Clambake - Operation Clambake is the title of a World Wide Web page that has become known as the single most important site with information about Scientology. It is run by Andreas Heldal-Lund, a critic of Scientology who views the organization as a cult. The Web site provides considerable insight into the workings of Scientology, and it includes links to Scientology's "secret" documents as well as other information that the organization has tried to suppress. The Web site is one of the focus points of the war between Scientology and the Internet. Scientology had made numerous legal threats to various Internet service providers that have hosted the site, demanding that it be removed from the Internet. In various incidents that have been documented in such publications as the New York Times, Slashdot and Wired Online, Scientology has also used copyright law to force notable Web sites (including the Google search engine) to remove all references to the Operation Clambake site.

Peer-to-peer - As opposed to non-peer or client-server. Peer-to-peer describes a symmetric protocol, application, or network where every node has equivalent capabilities and privileges. Any node is able to initiate or complete any supported transaction. Peer nodes may differ in local configuration, processing speed, network bandwidth, and storage quantity. A protocol can be categorized as peer (symmetric), non-peer (asymmetric, usually client-server), or both. Consider the Usenet news service. Usenet news servers are NNTP peers among themselves, but NNTP servers to Usenet newsreaders. Usenet newsreaders are NNTP clients to the Usenet servers but do not communicate with other Usenet clients directly. Usenet clients and servers implement only the portions of NNTP that are needed for their purpose.

PICS - Platform for Internet Content Selection; The PICS specification enables labels (metadata) to be associated with Internet content. It was originally designed to help parents and teachers control what children access on the Internet, but it also facilitates other uses for labels, including code signing and privacy

Scientology - Scientology is a controversial system of beliefs and teachings, begun in 1952 by author L. Ron Hubbard, and presented as a religion. It was first incorporated in the US as a Nonprofit Organization in

1954, and is considered to be a religious nonprofit organization under the tax code administered by the Internal Revenue Service. It is not a recognised religion in many countries, and in some countries, notably Germany, it is officially seen as a dangerous practice.

Search Engine - A search engine is a program designed to help the user access files stored on a computer, for example on the World Wide Web, by allowing the user to ask for documents meeting certain criteria (typically those containing a given word or phrase) and retrieving files that match those criteria. Unlike an index document that organizes files in a predetermined way, a search engine looks for files only after the user has entered search criteria. In the context of the Internet, search engines usually refer to the World Wide Web and not other protocols or areas. Because the data collection is automated, they are distinguished from Web directories, which are maintained by people.

Software cracking - Software cracking is software hacking in order to remove encoded copyright protection. Distribution of cracked software (warez) is generally an illegal (or more recently, criminal) act of copyright infringement.

SMS - Short Message Service (SMS) is a service made available on most digital mobile phones that permits the sending of short messages (also known as text messages) between mobile phones. SMS was originally designed as part of the GSM digital mobile phone standard, but is now available on a wide range of networks, including forthcoming 3G networks.

Software-patch - A software release is to create a new version of the system or program and release it to the user community. Each time a software system or program is changed, the programmers and company doing the work decide how to distribute the changes or the the changed system or program to those people using it. A software patch is a method of distributing the changes. It is either a program that modifies the original unchanged system or program to create the new one or a list of instructions for a person who follows them to create a new one.

Software-piracy - The term software piracy refers to copyright violation for profit, i.e., the unauthorised selling of counterfeit computer software, music, movies etc. The copying of software, music and films where no money changes hands, sometimes known as warez, is legal in some jurisdictions. In Russia, it is legal to copy any software as long as it is not in the Russian language.

Steganography - Steganography is the science of writing hidden messages, where "hidden" means not only that the message cannot be read by anyone other than the intended recipient, but also that no one else even knows that a message has been sent. Generally a steganographic message will appear to be something else, like a shopping list, an article, a picture, or some other "cover" message.

Spamming - Spamming is the process of sending unwanted electronic messages. The most common form of spam is Unsolicited Commercial Email (UCE) or Unsolicited Bulk Email (UBE), the electronic form of junk mail. A spammer will send identical or nearly identical messages to a large number of email addresses, often harvested from Usenet postings or web pages, or obtained from databases, without the permission of the recipients.

Streaming media - Streaming media is a term that describes "just in time" delivery of multimedia information. It's typically applied to compressed multimedia formats delivered over the Internet.

The Web - The World Wide Web ("the Web" or "WWW" for short) is a hypertext system that operates over the Internet. To view the information, one uses a piece of software called a web browser to retrieve pieces of information (called "documents" or "web pages") from web servers (or "sites") and display them on the user's screen. The user can then follow hyperlinks on the page to other documents or even send information back to the server to interact with it. The act of following hyperlinks is often called "surfing" the web.

Traffic - The information moved over a communication channel.

URL - A Uniform Resource Locator, or URL, is a standardized address for some resource (such as a document or image) on the Internet. First created by Tim Berners-Lee for use on the World Wide Web, the currently used forms are detailed by IETF standard RFC 2396 (1998).

Usenet - Usenet (also known as Netnews) is a set of protocols for generating, storing and retrieving news "articles" (which resemble mail messages) and for exchanging them amongst a readership which is potentially widely distributed. It is organized around newsgroups, with each newsgroup carrying articles about a specific topic. Readers see all the articles posted to each newsgroup in which they participate. These protocols most commonly use a flooding algorithm which propagates copies throughout a network of

participating servers. Typically, only one copy is stored per server, and each server makes it available on demand to readers able to access that server. Usenet was thus one of the first peer-to-peer applications.

Webcam - A webcam is a small digital camera attached to any computer that is connected to the Internet. It is mainly used to take pictures and make short films of the surrounding area or the camera's owner and post them in (almost) real time to the World Wide Web. Other uses might include chatting, security, and video conferences over the Internet.

Web Log - A web log (also known as a *blog*) is a website that tracks headlines and articles from other websites. They are frequently maintained by volunteers and are typically devoted to a specific audience or topic.

About the Author

As co-founder of the Dutch Internet service provider XS4ALL, Felipe Rodriquez has been at the center of the legal debate over censorship and Internet service provider issues in Europe and the world. Mr. Rodriquez founded XS4ALL in 1993, and acted as its CEO until 1997. In his role as CEO, Mr. Rodriquez was involved in a number of high-profile disputes concerning Internet politics. He took a stand in favor of protecting online civil liberties concerning material hosted on XS4ALL's server, and the successive court cases shaped the legal debate in the Netherlands on ISP liability.

In 1995, he created the Dutch ISP Industry Association, NLIP, and chaired it until 1997. As a representative of the Dutch Internet Industry association he participated in the EU commission roundtable discussion about harmful and illegal content on the Internet.

In 1996, he conceived and initiated the first Internet hotline (www.meldpunt.org) to combat the distribution of child pornography on the Internet; the Hotline was opened by the Dutch minister of justice, Winnie Sorgdrager, on the 20th of June 1996.

He also worked together with Belgrade radio station B92 to broadcast its radio signal live on the Internet after it was censored by the Milosevic regime. In 1997 Mr. Rodriguez led XS4ALL through another Internet issue that grabbed global headlines when German ISP's tried to block XS4ALL's servers because it hosted a homepage of the radical-left magazine Radikal which is illegal in Germany; the German actions failed as they resulted in a rapid worldwide mirroring of the page by Internet users.

XS4ALL was sold to Dutch Telecom Company, KPN, in December 1998. Rodriquez is currently on the advisory board of XS4ALL, and is a non-executive director of Maptive BV, Care4Cure BV, IF Media Ltd, Holotype Ltd and Conscious Investor Ltd. Rodriquez is a boardmember of bridges.org.