PORGMUN Research Paper

CREATING A UNIVERSALLY OPEN INTERNET: PREVENTING CENSORSHIP IN TOTALITARIAN REGIMES AND DURING POLITICAL CRISES

Introduction

The idea behind the Internet was to create an open and free communication channel that would be easily accessible from different parts of the world. It soon became an inseparable part of humanity, a source of shared knowledge as well as one of the major communication platforms. However, the open and free theme seems to be on the verge of collapse. Why? The reasons behind this are fairly straightforward.

Whilst being free and open today, this platform can also be easily abused. Nowadays we're facing the fact that this useful communication platform is used by terrorist organizations such as Al-Qaeda, to promote extremism, child pornography, and cyberbullying as well as to distribute pirated content freely over the Internet. The question arises: How should we effectively counter this threat and apply laws of our society on the Internet without possibly abusing human privacy or censoring content?

Piracy

For many reasons that were already mentioned, the Internet also represents a convenient way of distribution of pirated content worldwide. Pirated content is content, which is protected by copyright law; however it is distributed without permission. In the case of music/movie piracy, the losses caused by piracy can reach up to millions of dollars.

The most popular way to distribute pirated content nowadays is the use of peer-to-peer networks. It is convenient for both the copyright violators and

the people that demand the copyrighted works as this system involves sharing in between the data in between the subjects, so no distributor can be then found.

One of the most popular servers that provided this model was The Pirate Bay, which was raided by Swedish Police in December 2014. Nevertheless, this raid didn't stop the website from working and its several copies provided by another major peer-to-peer (aka. Torrent) websites isoHunt and KickAssTorrents went online in a matter of days. These sites are actively being censored or banned in many countries through Internet Service Providers. However, these actions didn't have any real effect on the current situation; because still over 100 million IP addresses perform peer-to-peer downloads every day.
Further research:
http://www.go-gulf.com/blog/online-piracy/
http://www.dailytech.com/Nearly+Half+of+Americans+Pirate+Casually+But+Pirates+Purchase+More+Legal+Content/article29702.htm

Terrorism over the Internet

The use of such a powerful tool as the Internet called for a current trend of integrating the Internet into your daily routine. With the same ease as you now use communication channels such as Facebook or WhatsApp, the terrorists of today have also become more advanced and began using the Internet as a sophisticated, reliable and far safer way of communication and publishing of propaganda. Their secret chatrooms and email "dead drops" make it very difficult for Law Enforcement units to eavesdrop their communication, not to mention attempting to trace the subjects suspected of terrorism. Terrorist propaganda or the videos of executions posted on the terrorists' websites attract potential new Jihadists from all over the globe. These websites also provide thorough tutorials that cover a wide variety of topics including those like how to create an improvised explosive device or how to cross the Iraqi borders. For example, one of the greatest powers of ISIS nowadays is its ability to attract jihadists to fight against western nations and to inspire them to prepare an attack inside the countries using social media, and other internet options.
Further research:
http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005
http://www.bbc.com/news/world-24784756

http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Current solutions to the issues:
Mass Surveillance to counter terrorism

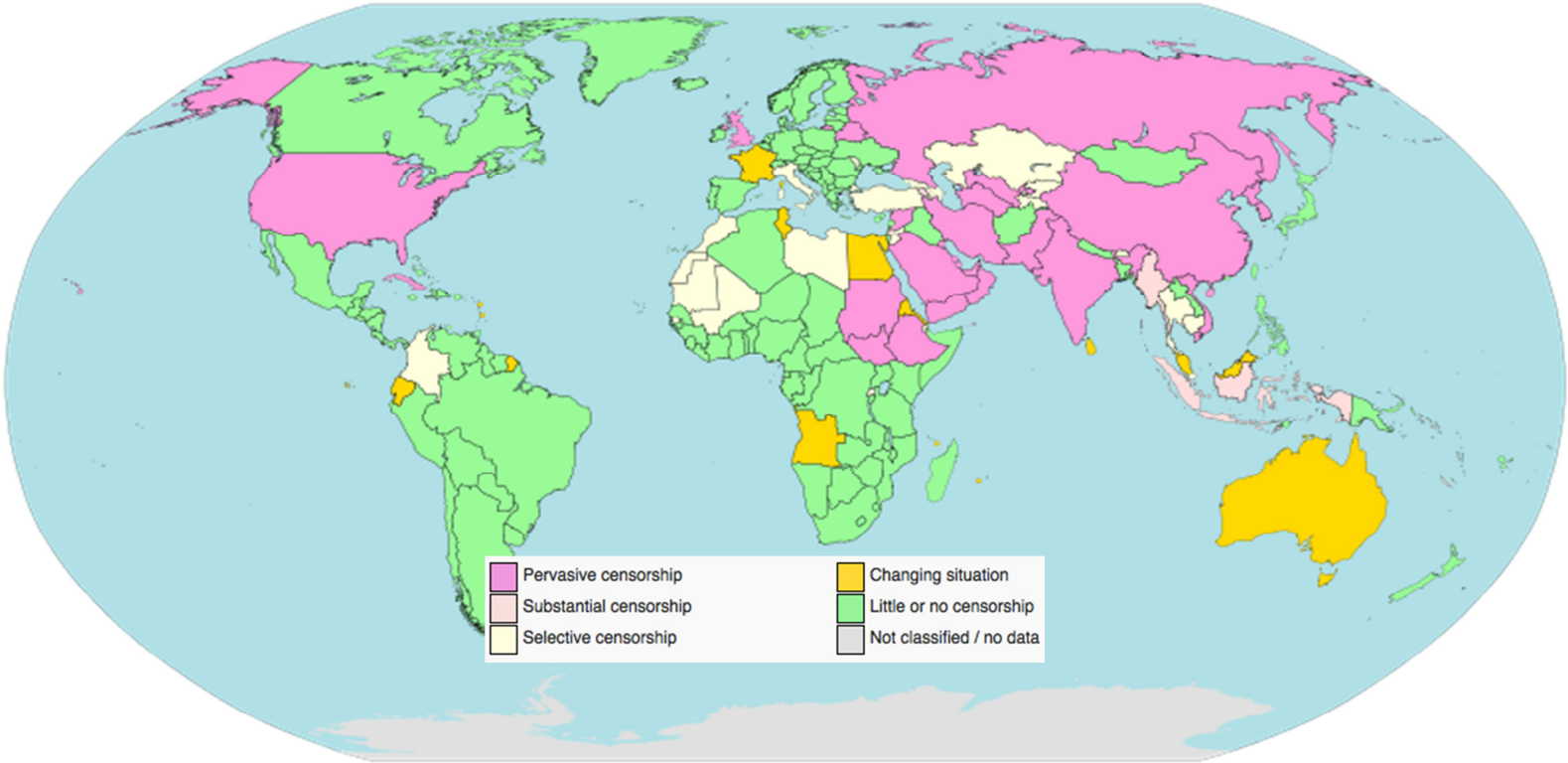
Some governments decided to step up their effort to counter the terrorist threat and started their own internet surveillance programs. The widely known example could be the PRISM program, which stands for clandestine anti-terrorism mass electronic surveillance data mining program. The program was launched in 2007 by US National Security Agency (NSA) to collect private electronic data belonging to users of major internet services. It used the legal authority gained from the Patriot Act as well as the Foreign Intelligence Surveillance Act (FISA). Under the program data was gathered from servers of major US based companies such as Microsoft, Yahoo!, Facebook, Google, PalTalk, AOL, Skype, Dropbox, Apple and countless others. Sophisticated analysis tools were used to automatically identify possible communication among potential terrorist organizations, as well as individuals, in order to prevent any terrorist attacks or other threats to the security, such as drug smuggling or trafficking. The potentially useful data is then being saved. However strictly classified, information about this program leaked due to a whistleblower and former intelligence contractor Edward Snowden. In the weeks since the PRISM documents leaked, a widespread international public debate about the United States government's surveillance and spying programs has engulfed the NSA, Congress, and the Obama administration in controversy. After this program leaked, the question arose: "Is the sacrifice your privacy for better security is acceptable?" It also must be added that this program is not the only one as more have been set up by NSA in cooperation with CGHQ such as ECHELON, MUSCULAR, DISHFIRE, STATEROOM and many more.

Further research:
http://gizmodo.com/what-is-prism-511875267
http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet
http://www.theguardian.com/us-news/edward-snowden

Internet censorship

Where is the difference between freedom of expression and unacceptable content? The approach of the countries to the freedom of expression varies greatly. While some of them propose the complete openness of the Internet, many countries decided to censor some websites, thus preventing their

content to be viewed. This may include websites distributing child pornography, pirated content, websites that encourage extremism, gambling, xenophobia, promoting criminal activity or terrorist websites. However, restricting access to some of these websites might have been more controversial. This is the case of many political blogs, opposition's or anti-regime protesters' websites or major servers, which operate with leaked sensitive internal communication and data (like WikiLeaks) that supposedly pose a security threat to the US. Massive acts of censorship also appeared during the Arab Spring, when the Internet went down for months in order to restrict access to protesters, who were organized mainly via Facebook.
The image below illustrates the level of censorship in the by individual countries.



One of the most rigorous Internet censorship systems is present in China, where government blocks websites that discuss the Dalai Lama, or the 1989 crackdown on Tiananmen Square protesters. The government also blocks many broadly used websites such as Facebook, Twitter, Google or YouTube. Same restrictions are also applied in countries like Iran and other Islamic countries.
Further research:

https://cyber.law.harvard.edu/pubrelease/internet-control/

Controversy:
Privacy

Today we live in a fully digitalized age, where we use credit cards or online banking, to perform payments, or email to send and receive important messages. We have Facebook, Twitter or Instagram accounts, where we share our private and personal information with our friends. We use Messenger, WhatsApp, iMessage or SMS chat with our friends. Our smartphones constantly upload our current location. Many of our important documents and other files are saved using cloud services such as Microsoft SkyDrive, Apple iCloudDrive, Dropbox or Google Drive. Imagine, that someone would be granted full access to all of this information. Access to information, which follows your every move, follows every aspect of your personal life and your work. With systems as PRISM your personal information, emails, location can be easily accessed, stored and viewed by more than 800 thousand government officers without any need for court approval or your permission. It was initially designed to pursue subjects suspected of terrorism, but who is in charge of controlling whether it isn't misused. Does any government have a right to limit or pursue their citizens, even though it's done to prevent terrorist attacks?

Your task

You'll be asked to think of solution to the censorship of the Internet, while trying to prevent terrorism and piracy that happens over the Internet. You also have to keep in mind that ignoring the privacy of your citizens may also be badly received by public. It's up to your country's preferences whether, how and to what extent would your country like to make the Internet a better place. Put an emphasis on what your country's preference is as you're not representing yourself but your country.

Sources

http://www.go-gulf.com/blog/online-piracy/
http://www.dailytech.com/Nearly+Half+of+Americans+Pirate+Casually+But+Pirates+Purchase+More+Legal+Content/article29702.htm
http://gizmodo.com/what-is-prism-511875267
http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

http://www.theguardian.com/us-news/edward-snowden
https://cyber.law.harvard.edu/pubrelease/internet-control/
http://en.wikipedia.org/wiki/Censorship
http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005
http://www.bbc.com/news/world-24784756
http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf