International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 10, Issue 2, 2024, PP 22-30
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
https://doi.org/10.20431/2349-4859.1002002
www.arcjournals.org

Internet Censorship and its Implication on Personal Privacy

E.N EKWONWUNE[1], A.EDUROHA[2], M.C. DENNIS[3], U.C CHIGOZIE[4]

[1,4]Department of Computer science, Imo State University, Nigeria
[2]Department of Computer Science, Gregory University, Nigeria
[3]Department of Computer Science, The Polythecnic Nekede, Nigeria

Corresponding Author:** ***E.N EKWONWUNE, *Department of Computer science, Imo State University, Nigeria*

Abstract: *The internet as a global market place has revolutionized the way we communicate, access information, and conduct business. It has become an essential tool for billions of people around the world. The rapid development of the Internet and especially of Internet-based commerce and other forms of activities has largely taken place outside the standard trade-regulatory frameworks that cover most other forms of cross-border commerce. However, as the internet has grown in importance, so has the debate over internet censorship, content filtration and the need for net neutrality and the attendant implications on personal privacy? This paper again looked at the arguments on the concept of internet censorship whether the, legality, morality or otherwise and how it affects us positively or negatively most importantly the who, how and why. Again, ordinary least square method was adopted for the analysis on some of the objectives of this paper including establishing a relationship between crime rate and internet censorship.*

Keywords: *Internet, Internet Censorship, Security, Conflicts, Crime, Censorship, Data.*

1. INTRODUCTION

Some countries censor the internet because they don't want their citizens to see things that might upset them or make them think differently. They also might do this to keep people from organizing protests or speaking out against the government. Their goal, usually, is to make it difficult to get accurate information about what's going on in the world or stop people from being able to share their opinions freely.

Internet censorship refers to the practice of controlling what people can access or publish on the internet. Governments, corporations, and other organizations can use a variety of methods to censor the internet, including blocking websites, filtering content, and monitoring online activity. The reasons for internet censorship can vary, from protecting national security to preventing access to harmful content such as pornography or hate speech. While some argue that internet censorship is necessary to maintain social order and protect citizens, others believe that it is a violation of freedom of speech and expression. Censorship of the internet happens in one of two directions:

1. **Top-down censorship** is when a government or organization tells service providers what content to block. In some cases, laws may require certain content to be censored. Users have no say in this and can't choose what to access.
2. **Self-imposed censorship** is associated with individuals or groups self-censoring by choosing what content to avoid. For example, someone may decide not to view certain websites because they know their government will censor the information, making it inaccurate.

Net neutrality, on the other hand, is the principle that all internet traffic should be treated equally, regardless of its source, destination, or content. Net neutrality means that internet service providers (ISPs) should not be able to discriminate against or favor certain websites, applications, or services. For example, an ISP should not be able to slow down or block access to a website that competes with one of their own services. Net neutrality is important because it promotes competition and innovation, encourages free expression and access to information, and prevents ISPs from exerting too much control over the internet.

2. Statement of problem

The Internet has made it easier for individuals to access any information they want, and hence Internet Censorship is applied to filter contents that are deemed negative.

The problem arises from the simple fact that Internet does not respect national boundaries and online services provided at one point on the globe can, in principle, be accessed at any other point. Governments, who prefer that particular pieces of information of services should remain inaccessible from the population, are unable to act outside its jurisdiction using traditional means of enforcement: Anyone, with little or no means, to have an instant global reach without traditional market-entry barriers like physical investments, distributors, real estate, and infrastructure – and more importantly all the regulatory instruments (such as permits, licences and supervision) that are based upon them.

3. Aim and Objectives

The main aim of this paper is to ascertain the real impact and implication of internet censorship on personal privacy. This can be achieved with the following

i. X raying the different methods and strategies of censorship

ii. Implications and applications of internet censorship on economy

iii. Internet censorship and crime rate

4. Literature Review

Internet censorship refers to the act of filtering and controlling what can be accessed on the Internet, usually done by the government to control the public. There are several approaches to Internet censoring (OpenNet. 2013)

***Technical Blocking*;** Technical Blocking simply refers to the act of blocking access to Internet sites such as IP blocking, DNS tampering, and URL blocking using a proxy. This also includes keyword blocking, which is a method used to block access to sites that have specific words in their URLs.

***Search Result Removals*;** Search Result Removals is a common censorship approach applied by Internet search engines such as Google and Yahoo. Instead of blocking access to specific sites, this approach makes finding them much more difficult. In many cases, this is used to make finding pirated contents much harder to do.

Takedown; The takedown approach simply demands specific sites to be removed from the Internet.

Induced Self-censorship; In many cases, individuals will stay away from several websites that may question the authorities, even when these sites are not restricted e.g. porn sites that include child pornography. Furthermore, (OpenNet. 2013) Internet censorship into four types based on their themes:

***Political Internet Censorship*;** Political Internet Censorship includes censoring contents related to views that oppose the current political regime. Censorship regarding to contents related to human rights, minority rights, religious movements and freedom of speech are also included in this group. Countries with high-level Political Internet Censorship include Vietnam and Uzbekistan.

***Social Internet Censorship*;** Social Internet Censorship includes censoring contents that are deemed inappropriate by several religious or political groups, such as pornography, violent materials, gambling websites and any other contents that may not be suitable for children. Countries with high-level Social Internet Censorship include Saudi Arabia and United Arab Emirates.

***Conflict (Security) Internet Censorship*;** Conflict Internet Censorship deals with contents including separatist movements, border issues and any other military movements that may jeopardize the security and safety of the country. Countries with highlevel Conflict Internet Censorship include China and South Korea.

***Internet Tools Censorship*;** Internet Tools Censorship covers blocking and censoring tools that are used by Internet users such as e-mail, Internet hosting, translation, search engines and any other communication tools that use the Internet. Countries with high-level Internet Tools Censorship include Saudi Arabia and United Arab Emirates.

4.1. Advantages and Disadvantages of Internet Censorship

The debate in censorship has never been resolved, and it only amplifies after the introduction of the Internet. There are several advantages of Internet censorship:

i. It protects individuals from incorrect and biased information. According to S. Colaric, (2009) there is no sufficient evidence to suggest that children can differentiate credible information from non-credible ones. This can be dangerous as biased and incorrect information can affect a child’s perspective in a very significant way.

ii. It protects individuals from contents that can be deemed inappropriate such as pornography. Besides religious and ethical reasons, pornography may have negative impacts towards young men and women, as they are more likely to engage in risky sexual behaviors when they are exposed to high-level of pornography (A. J. Bridges 2009)

iii. It battles piracy by blocking contents that may violate intellectual property rights.

iv. It protects individuals from online scams.

v. It can protect individuals from cyber-bullying, cyber-racism, cyber homophobia and cybersexism (OAIC. (2013, September)

However, Internet censorship is not without any disadvantages. Some of these disadvantages include:

i. It limits freedom of speech. According to D. Charoen, 2012, the Computer Crime Act in Thailand has been criticized for its excessive Internet censorship.

ii. It gives government too much power and control over information. This has been considered as a huge issue in China, as it may delay the radical change that China needs (Ref. [6]).

4.2. How Internet Censorship May Relate to Crime Rate

The possible relationship between Internet censorship and crime rate stems from the relationship between crime rate and media censorship in general. The classical notion argued by most people is that violence and pornography in media have significant impacts on an individual’s violent behavior. However, a study by C. J. Ferguson, 2009, concluded that there is no sufficient evidence to suggest any relationship between media violence effects and violent crime. Furthermore C. J. Ferguson and R. D. Hartley, 2009] argued that pornography does not lead to an increase in violent sexual behavior. The Internet takes information sharing to a different level, and its introduction to the public makes media censorship so much more complicated. With the Internet, any individual can access any information they want, and without any restrictions these information include child pornography, drug market and any other contents that are not only deemed inappropriate but are also expected to increase criminal intent. Along with Internet usage, Internet censorship has also been increasing and it is gaining attention from scholars from different disciplines such as media and communication, information technology, law, political science.

4.3. Motivations for Censorship

As censorship as a phenomenon is as old as civilisation itself, it is hardly surprising that the motivations and targets of online censorship are not markedly different from those that affect other media.

The political motivation, to curb critical ideas, opposition groups and regime criticism, is common. Internet traffic is rigorously monitored and critical sites based overseas blocked in many countries, including, among others, China, Iran, Maldives, Myanmar, North Korea, Syria, Tunisia, Turkey, Uzbekistan, Vietnam to mention a few. In Cuba, accessing the Internet is per se an illegal act, without the proper official permits. Subject for political censorship could also be ethnic orarmed conflicts. In China for example, information relating to Falun Gong, Taiwan, Tiananmen Square or the Tibetan independence movement are blocked. Information about North Korea is routinely censored in South Korea. Law enforcement agencies in Russia and other CIS countries have been given powers to fully monitor all Internet activities following the experiences in Ukraine and Georgia, where the opposition successfully utilized modern communications to start popular revolts. Political figureheads are sensitive subjects too – popular services such as the streaming video service YouTube and blogging services have been shut down in Turkey for defaming Kemal Atatürk, the founding father of the republic. Similarly, criticism of the King, lèse majesté, is forbidden in Thailand online as well as offline (and is often used to prosecute the opposition). French and German laws against glorification of Nazism and holocaust denial are upheld online against sites hosted overseas, whereas enjoying sometimes constitutional protection in other countries.

Second motivation for censorship is for moral reasons, based on what societies perceive as immoral or illegal. Examples of such are numerous, and usually concern pornography, gambling or criminal activities. Moral censorship on more secular grounds also exists: in the United States, online gambling is illegal though the sites are not blocked. Most countries (including those who do not practice censorship per se) block sites offering child pornography.

*A third motive***,** albeit more rare, is for commercial purposes. The most prominent example is Mexico, where the former state-owned operator, Telmex, blocked Internet-based carriers such as Skype and Vonage, providing an inexpensive voice-over IP (VoIP) services

4.4. How does Internet Censorship Work?

Censors employ technical methods to block its internet users from accessing a selection of websites (such as foreign news sites), apps (like Facebook and YouTube), and services (like Google). In some cases, countries enact laws that make it difficult to publish content to the internet. In extreme cases, they deny citizens access to the internet altogether Internet censorship can take on many forms. Internet censorship is not restricted to just one thing but encompasses a combination of the following.

DNS: The most common and primitive tool to censor websites and services is to redirect DNS records. This is akin to removing a business from a phone book or maps service, though it will still allow those familiar with the service to reach it directly. A common circumvention method for this strategy is to use a DNS provider outside of your home jurisdiction, as foreign providers would not comply with the censorship request.

IP block: A more sophisticated strategy is to block all requests and connections with IP addresses connected to the target site. If the blocked site is hosted on a shared server, then all the sites on that server will face the same fate.

Deep Packet Inspection: Deep packet inspection (DPI) refers to the process of analyzing every single piece of data going in and out of a restricted network. It requires massive resources, as powerful computers and storage units have to be erected at every digital border. As a side effect, connections will appear considerably slower.

Speed Malfunctions: Some corporations might throttle your internet connection and make it incredibly slow and cumbersome to reach certain sites. This approach has been used by ISPs in the past to restrict access to peer-to-peer sites such as uTorrent and LimeWire.

4.5. How Censorship Works in Different Countries

Some countries have rigid censorship laws, while others have none at all. China is well-known for its internet restrictions, which some call the “great firewall of China.” The Chinese government blocks access to many websites and social media platforms, like Facebook and Twitter. Google’s search engine, as well as all other Google products, is also banned in China. The government is censoring search results and blocks certain words from being used online.

In Saudi Arabia, the government filters content based on religious and moral values. It usually blocks websites that contain pornography or material that could be considered offensive to Islam. In Iran, the government blocks websites that are critical of the regime or that contain information that could be used to foment dissent.

In Russia, a new law requires internet service providers to censor websites that the government decides are “extremist.” This can include foreign websites that have critical opinions of the government in question or that provide information about protests or other forms of defiance.

4.6. Internet Censorship Issues: How does it Affect us?

Skewed Worldview: Censorship influences how we understand the world and society, often by presenting a more positive picture of one’s own society. It also prevents us from knowing about alternate ways of life around the world.

Inconvenience: It can be frustrating if the main online services you use are blocked when you're traveling or living abroad. This could mean you must go without your main email, messaging apps, social media, and video chat tools that you rely on to stay in touch with family and friends, and for news and entertainment.

Business Disadvantages: Companies are hampered by censorship when they don't have access to all the information that could help them make business decisions.

Loss of Privacy: In high-censorship countries, individuals are limited to using a set of locally available social media and chat apps, and those apps are likely monitored for sensitive content, which gets removed before it can be widely disseminated.

Edited Entertainment: A country might block streaming services or certain films and TV shows, or only permit versions that cut out content that runs counter to its preferred messaging.

4.7. How to Circumvent Censorship

If you live in a country with restricted internet, there are several ways to bypass the restrictions and gain access to all internet content.

Proxy

Web proxies are the simplest, fastest way to get around censorship and regional restrictions on the internet. They work by routing your traffic through a different server so that the website you are trying to visit doesn't know your true IP address. This can be used to get around simple content filters, like the ones your school or workplace may have in place.

Web proxies are not perfect, however. They can be slow, and they don't always work with every website. Additionally, your traffic is still going through another server, which means that the proxy owner could be snooping on your traffic and detecting phony IP addresses. More important – your internet service provider and, thus, the government, can still know what you were browsing.

VPN

Another way to get access to censored websites is to use a virtual private network. VPNs create a private, secure connection between two devices, which can be used to access restricted websites. When you use a VPN that doesn't log data, your traffic is encrypted, so your ISP or anyone else can't see what you're doing online. Even more important, there's no data saved on the provider's side as if you've never used the service at all.

While VPNs are legal in most parts of the world, some countries block them and can even issue a fine if you get caught. If you're using a VPN in a country where they are not allowed or just worried about the repercussions, you may need to use a different method to access restricted websites.

Tor Browser

Lastly, you might only need to switch your internet browser to a more secure one. Tor is a free browser that allows you to surf the internet anonymously. By encrypting traffic and bouncing it through a distributed network of relays, Tor makes it difficult for anyone to track a user's online activity.

The main downside to using Tor is that it can be slow. Because traffic is routed through multiple relays, each with its own bandwidth limitations, Tor users may experience slowdowns when browsing the web. Additionally, some websites may block traffic from known Tor relays, making them inaccessible to Tor users.

4.8. Why Internet Censorship is Good

Prudence

Most users have the decency and common sense not to post something online that society would consider unhealthy or inappropriate content. The key here is "most users". Internet users come in all varieties. If you visit Google (without filters enabled) there are some gory videos depicting murders and other high-level crimes, including information related to Illicit drugs, Sexual assault, Sex trafficking, Identity theft., Threats to law enforcement agencies and personnel. Internet censorship methods are implemented to make accessing these sites more difficult. These measures included a question prompt when entering websites “Are you 18 years or older?”

National Security

Government agencies know that information sharing on the web can threaten national security. Sensitive content, including numerous videos of military movements and tactics, posts about proprietary economic information, or other compromising details can put our country at risk. Although the United States is often thought to be the home of absolute freedom, internet censorship takes on a very real purpose when it used to protect the national economy or other factors that can influence our position on the global market.

Limits Child Pornography and Other Harmful Information

Law enforcement agencies worldwide have spearheaded efforts to restrict access to harmful or false information. By restricting access to this content through direct censorship, local authorities and government organizations place common sense limits on the type of content available.

Minimizes Risk of Identity Theft and Other Cyber Threats

Cybercrimes are a rising concern in this digital era. People store a lot of their personal and private information on their computers. Without the proper knowledge of passwords and privacy policies, users can leave themselves very vulnerable online. Limiting the amount of information put online can certainly assist in minimizing the threat of these cyber attacks. If internet censorship is designed to prevent access to the tools and strategies used to commit cyber crimes, communities must weigh the advantages and disadvantages of such regulation.

Eliminates Misleading/Fake News

With news media sites springing up all over the web, it can be hard to know what is real and what is fake news. Established news outlets like CNN, Fox, and CNBC are not the only players on the web anymore. With the end-goal of profiting only, there are many sites in existence that cash in on providing false, misleading articles online.

By enacting a strong program of internet censorship, this censorship could most likely reduce the amount of fake news. Over the past few election cycles, the sharing of fake news on social media has presented significant challenges. The pros and cons of free speech regulated on social media balance the ability to access information while limiting the spread of potentially harmful — or false — news.

Protects Privacy Censorship programs online provide many benefits, especially if you are struggling with access to violent material, negative information, or harmful content. Online censorship typically cleans that up for you automatically. This also goes for illegal activities and anything that goes against freedom of speech in general. There are several advantages to using automated internet censorship tools, particularly those that target specific websites known for trafficking in false information. More importantly, there are times when personal information is leaked to the web.

4.9. Why Internet Censorship is Bad

Amnesty International together with The Observer and Soda Creative launched a campaign called *irrepressible. Info* against the increasing governmental censorship of the internet. The campaign asks governments to stop censoring websites, blocking emails or shutting down blogs and make an appeal to the big corporations to stop supporting these actions. Private organizations that champion freedom of speech argue that internet censorship creates an unfair playing field — one that can have serious and long-term ramifications regarding freedom. Some of the disadvantages of internet censorship include:

Decrease in the Flow of Information

The amount of factual and real news that is published online will be severely limited when internet censorship is implemented. There are individuals arrested each and every day for sharing inappropriate and illegal content online. Even liking a post on Facebook or commenting on a blog post can land you in a heap of legal trouble.

Expensive

Regarding the disadvantages of internet censorship, one of the most notable cons of censorship is the cost. It costs money for monitoring the internet. Google has over 2.1 trillion results; with this huge volume of results, it would require a costly process to filter all of the information published online. Many people are all in favor of internet censorship until they realize it will raise their taxes. Financial considerations are always at the forefront of any attempt to clamp down on open internet speech — many an oversight entity has reconsidered its position after seeing the price tag associated with censoring material on the web.

Negative Impact on the Economy

Nowadays there are more and more entrepreneurs born into our economy. With the highest number of startup companies in history, it is important that these businesses can freely promote themselves. The internet has become a primary economic driver, and that is the result of the free exchange of information. Increasing internet censorship could have devastating consequences for local businesses, potentially locking them out of economic opportunities. By losing the freedom to sell your products online, the result may have dire effects on the nation’s economy.

Minimizes Entrepreneurial Efforts

Wrapping up the disadvantages of internet censorship, the whole idea of being an entrepreneur is having the freedom to create and sell anything. Once there is a governing body acting as a mediator, it limits what you can actually do and how successful you will be. The internet may no longer be a viable tool for creating wealth, especially if censorship derails the free exchange of information.

The best example of this would be Nike if you wanted to start your own athletic apparel company it could be nearly impossible. Nike has the wealth and branding power to completely wipe you off of the grid. As a result, internet censorship here would greatly limit the increased flow of innovation. Then end result of this move may result in many monopolies across every industry, with each monopoly positioned due to the loss of free information access.

5. Methodology

Using OLS: Possible Endogeneity Problem

One way to estimate the relationship between Internet censorship and crime rate is by using OrdinaryLeast Squares (OLS). Consider the following equation:

$$crime_i = \beta 0 + \beta 1 \cdot conflict_i + \beta 2 \cdot political_i + \beta 3 \cdot social_i + \beta 4 \cdot tools_i + e_i \qquad , (1)$$

Where

$crime_i$ is the crime rate in country i,

$conflict_i$is the level of conflict Internet censorship in country $_i$,

$political_i$ is the level of political Internet censorship in country $_i$,

$social_i$ is the level of social Internet censorship in country $_i$,

$tools_i$ is the level of Internet tools censorship in country $_i$ and e_i captures all unobserved influences on crime rate in Eq. (1).

In order to consistently estimate Eq. (1), the error term e_i must not be correlated with any of the regressors in the equation.

If e_i is correlated to any of the regressors in Eq. (1), then the correlated regressors are endogenous in the equation and their respective parameters will be biased.

For example, if $conflict_i$ is correlated with e_i in the equation, then $conflict_i$ is endogenous in the equation and β1 is biased. When the parameter is biased, any inferences and tests such as t-tests and F-tests will be invalid. Thus, OLS can only consistently estimate the parameters in Eq. (1) when all regressors in the equation are exogenous.

However, there are reasons to believe that the regressors in Eq. (1) may be endogenous:

i. Internet censorship is expected to be correlated with Internet penetration. When a country is more exposed to the Internet, there are many complications that come with it and hence it is normal for the government to pay more attention to media censorship. Furthermore, Bitso et al (2012) reported that Internet censorship has been increasing together with Internet penetration. Access to Internet may have an impact on crime rate, as the Internet makes it easier to obtain illegal weapons.

ii. A country's openness may be correlated with Internet censorship, as they both can represent a country's attitude towards other countries and global information. Such general behavior of a country may have an impact on its crime rate.

Furthermore, it is possible that Internet censorship may be correlated with other influences on crime rate such as economic growth, population and land area.

Taking these variables into account, we consider the following equation:

$$\boldsymbol{crime_i = \beta 0 + \beta 1 \cdot conflict_i + \beta 2 \cdot political_i + \beta 3 \cdot social_i + \beta 4 \cdot tools_i + \beta 5 \cdot internet\ penetration_i + \beta 6 \cdot gdp\ growth_i + \beta 7 \cdot land\ area_i + \beta 8 \cdot population_i + \beta 9 \cdot opennes_i + u_i} \qquad \textbf{(2)}$$

where internet penetration$_i$ is the number of internet users per 100 people in country $_i$, gdp growth$_i$ is the annual GDP growth of country i, land area$_i$ is the land area of country $_i$, populationis the population of country $_i$, openness$_i$ is the sum of exports and imports of goods and services measured as a share of GDP of country i and ui captures the unobserved influences on crime rate in Eq. (2).

6. Analysis

6.1. Data Description

In this paper, we are using a cross-sectional data set for the year of 2013, consisting of 60 countries; thus, i = 1, 2. . . 60.

The dependent variable, crimei is obtained from Numbeo. (2015). The crime index is an estimation of overall level of crime in a given country Numbeo. (2015)

It is used a proxy for a country's crime rate. The range for this variable is from 0 to 100. The Internet censorship variables conflict$_i$, political$_i$, social$_i$ and tools$_i$ are obtained from OpenNet. (2013). The value that these Internet censorship variables can take is either 0, 1, 2, 3 or 4.

The Internet censorship variables take a higher value as a country's level of Internet censorship becomes more intense. The Internet censorship variables take the value of 0 if there is no evidence of filtering. For example, conflict$_i$ = 0 when there is no evidence of Conflict Internet Censorship. The Internet censorship variables take the value of 1 if there is suspected filtering; that is when even though there is no confirmation of Internet censorship, there are connectivity problems that suggest its presence. For example, conflict$_i$ = 0 when there is evidence of Suspected Conflict Internet Censorship. The Internet Censorship variables take the value of 2 if there is selective filtering, that is censoring a few specific sites within a category or targeting a single category. For example, conflict$_i$ = 2 when there is evidence of Selective Conflict Internet Censorship. The Internet censorship variables take the value of 3 if there is substantial filtering, that is censoring several categories at a medium level or filtering many categories at a low level. For example, conflict$_i$ = 3 when there is evidence of Substantial Conflict Internet Censorship. The Internet censorship variables take the value of 4 if there is pervasive filtering, that is censoring sites at a high level, targeting a large portion of several categories. The Internet censorship variables conflict$_i$, political$_i$, social$_i$, and toolsi are measured by OpenNet. (2013) as ordinal, numerical variables. In this model, we are going to use them as they are. We considered transforming them into binary variables for each level of censorship, but we decided against it due to the following reasons. None of the 60 countries sampled have a censorship value of 1 that means none of the 60 countries have any evidence of suspected Internet censorship. Furthermore, the dummy variables together have a near singular matrix. If we transform each Internet censorship variables into binary variables, we are going to end up with 4× 4 = 16 variables or at least 3×4 = 12 variables if we do not add the Suspected Internet censorship variables. Since our sample size is only 60 countries, it is not a good idea to have too many variables as it would use too many of our degrees of freedom. Furthermore, we want to have enough degrees of freedom if we want to add more variables into the model. The Internet censorship variables are obtained from the same source (OpenNet. (2013)), and it is reasonable to assume the relationship between the levels of censorship to be approximately linear.

7. Summary and Conclusion

7.1. Summary

In summary, the main results that can be obtained from our analysis are of the following. There is no sufficient evidence to suggest that there is a causal relationship between political, social or tools Internet censorship and crime rate. There is sufficient evidence to suggest that conflict Internet censorship has a negative impact on crime rate for highly educated countries, but not for poorly educated countries. There is sufficient evidence to suggest that Internet penetration has negative impact on crime rate for highly educated countries, but not for poorly educated countries. However, there are limitations to our analysis in the following aspects. The data obtained may not be the correct proxy for the data we wanted. For example, the crime index calculated may not be the best overall estimate of a country's crime rate. Our sample size is only 60 countries because of the unavailability of the data. If we can get a larger sample size, we can make the models more efficient.

7.2. Conclusion

In conclusion, having clearly x rayed the concept of internet censorship, and how it affects us positively and negatively , and having seen how most countries have struggled with the factors that lead to censorship, and most countries continue to balance the advantages and disadvantages, it is important to note that;

i. Proponents of stifling the open exchange of ideas on the web often put security over freedom.

ii. Those fighting against web censorship argue that internet users should be able to make their own decisions about what can or cannot be posted online.

References

A. J. Bridges, "Pornography's eeffect on interpersonal relationships," Ph.D. dissertation, Department of Psychology, University of Arkansas, 2009.

J. Ferguson and R. D. Hartley, "The pleasure is momentary the expense damnable?:The influence of pornography on rape and sexual assault," Aggression and Violent Behavior, vol. 14, no. 5,pp. 323–329, 2009.

C. Bitso, I. Fourie, and T. J. Bothma, "Trends in transition from classical censorship to internet censorship: selected country overviews," Innovation: journal of appropriate librarianship and information work in Southern Africa: Information Ethics, no. 46, pp. 166–191, 2013.

J. Ferguson, Violent crime: Clinical and social implications. Sage Publications, 2009. Carolina Libraries, vol. 61, no. 1, p. 6, 2009.

Charoen, "The analysis of the computer crime act in thailand," International Journal of Information, vol. 2, no. 6, 2012.

Deibert, R. J., Palfrey, J. G., Rohozinski, R. & Zittrain, J. eds (2008), Access Denied: The Practice and Policy of Global Internet Filtering, MIT Press

E. B. Karnadi, "Does internet censorship reduce crime rate?," CommIT Journal, vol. 9, no. 1, pp. 35–44, 2015.

Economist, Ed., How Does China censor the Internet?, 2013, retrieved June 18, 2015.http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-china-censors-internet

Numbeo. (2015) About crime indices at this website, http://www.numbeo.com/crime/indices

OpenNet. (2013) (a) about filtering. Retrieved june 15, 2015, https/::opennet.net:about-filtering;research;

W. Bank. (2015) The world bank databank.: http://data.worldbank.org/indicator

Wu, Tim (2006), the World Trade Law of Internet Filtering, Columbia University Law School

Citation: *E.N EKWONWUNE et al. "Internet Censorship and its Implication on Personal Privacy" International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), vol 10, no. 2, 2024, pp. 22-30. DOI: https://doi.org/10.20431/2349-4859.1002002.*