Norges miljø- og biovitenskapelige universitet

Master's Thesis 2018 30 ECTS

Faculty of Landscape and Society
Supervisor: Kirsti Stuvøy

Internet or Bust: Market Driven Cybersecurity in the USA

Kyle Robert Knapp
MSc International Relations
Noragric

[BLANK PAGE]

Internet or Bust: Market Driven Cybersecurity in the USA

Kyle Robert Knapp
Ås, 2018

[BLANK PAGE]

The Department of International Environment and Development Studies, Noragric, is the international gateway for the Norwegian University of Life Sciences (NMBU). Established in 1986, Noragric's contribution to international development lies in the interface between research, education (Bachelor, Master and PhD programmes) and assignments.

The Noragric Master thesis are the final thesis submitted by students in order to fulfill the requirements under the Noragric Master programme "International Environmental Studies", "International Development Studies" and "International Relations".

kyknapp@gmail.com

Noragric Department of International Environment and Development Studies
The Faculty of Landscape and Society
P.O. Box 5003
N-1432 Ås
Norway
Tel.: +47 67 23 00 00
Internet: https://www.nmbu.no/fakultet/landsam/institutt/noragric

[BLANK PAGE]

Declaration

I, Kyle Robert Knapp, declare that this thesis is a result of my research investigations and findings. Sources of information other than my own have been acknowledged and a reference list has been appended. This work has not been previously submitted to any other university for award of any type of academic degree.

Signature……..…….
Date……13 December 2018……

[BLANK PAGE]

Acknowledgements

First and foremost, I would like to thank my supervisor Kirsti Stuvøy for her wisdom and support throughout the process of my thesis, and the trust she gave me. Her knowledge and insight into international relations proved to be invaluable as I explored my subject.

I would also like to thank Ragnhild Grønning for her love and support as I continue my education. I really couldn't have done this without her.

Thank you to my family for the love and support they have provided from halfway around the world.

Lastly I would like to thank the Norwegian government and the Norwegian University of Life Sciences in Ås, for accepting me as an international graduate student in the International Relations program. The coursework was challenging and engaging, and allowed me to grow as an individual. The passion of my professors did not go unnoticed.

[BLANK PAGE]

Abstract

The introduction of the internet has played a large role in how humans exist. From the way we conduct business, communicate, socialize and acquire information, no longer are we dependent on a geographical location to explore our world. However, with all of the good the Internet has brought us, our ability to access that data may be denied or hindered by business practices or limitation of physical infrastructure; creating inequalities on the net. During 2010 to 2017, the United States of America found net neutrality principles as a way to safeguard citizens. However this was reversed when in 2018 the Federal Communications Commission moved to dismantle those principles under the ruling *Restoring Internet Freedom*, instead looking to market to help drive security.

This thesis investigates the judgement of the Federal Communications Commission decision to implement the policy *Declaratory Ruling, Report and Order, and Order: Restoring Internet Freedom*. This policy rolls back Obama-era net neutrality measures that were implemented under *Open Internet Order* of 2010 and 2015. Asking the research: *How is the governing of internet access in the United States, as expressed in the new 2018 ruling, affecting citizens' security?*

From *Restoring Internet Freedom,* this thesis seeks to answer this question via a theoretical approach, utilizing securitization theory and an emancipatory practice to understand 'who are we securing?', 'from what threats?', and 'by what means?' The research is conducted by a qualitative document analysis method, utilizing the *Restoring Internet Freedom* as its primary document. This source is then compared to information gathered from secondary sources. The results from this study indicate that the ruling may pose a potential risk to citizen security, and places a greater interest in the welfare of businesses. The 2018 ruling removes net neutrality laws that were considered too heavy handed, and in place allows businesses to self-regulate. However these rules were in place as Internet Service Providers were digitally altering customer access, refusing to develop new or existing infrastructure, and practicing price discrimination.

[BLANK PAGE]

Table of Contents

[BLANK PAGE]

List of Abbreviations

AS	Autonomous System
CFR	Council on Foreign Relations
CSS	Critical Security Studies
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
DoC	Department of Commerce
ENISA	European Union Agency for Network and Information Security
EFF	Electronic Frontier Foundation
FCC	Federal Communications Commission
FTC	Federal Trade Commission
GAC	Governmental Advisory Committee
IANA	Internet Assigned Numbers Authority
ICAAN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IGF	Internet Governance Forum
IP	Internet Protocol
IRS	Internal Revenue Service
ISP	Internet Service Provider
NPRM	Notice of Proposed Rulemaking
OECD	Organization for Economic Co-operation and Development
PII	Personally Identifiable Information
QDA	Qualitative Document Analysis
SAE	Security As Emancipation
SLD	Second Level Domain
TLD	Top Level Domain
VPN	Virtual Private Network
WSIS	World Summit on the Information Society

[BLANK PAGE]

1. Introduction

The Internet today has created the ability for humans to advance themselves as never before, impacting the way we conduct business, disseminate information, collaborate, and communicate. Our lives are no longer bound geographically as the Internet can bridge societies and knowledge. What we wanted to know and discover is no longer constrained to the information that you were physically able to reach; instead it could be gathered at the click of a mouse. However, with all of the good the Internet has brought us, our ability to access that data may be denied by Internet Service Providers (ISPs) by their business practices or limitation of physical infrastructure. Showing that the system develops inequality as a byproduct, that the security of your data can be imposed upon by ISPs and access based on circumstance of your location or socioeconomic status.

ISPs provide the crucial work of developing physical infrastructure of the Internet, as well as offering the ability to connect into the data stream. However ISPs have been known in the past to manipulate customer data by throttling, blocking, or discrimination. (Stoltz and McSherry, 2017). Occurring under light-touch regulations, ISPs were operating legally per rules set under the Federal Communications Commission (FCC) *Telecommunications Act of 1996*. (Brotman, 2016). However as more citizens faced insecurities in equal access and use, the FCC moved to implement net-neutrality rules, culminating in the 2014 *Title II Order*, under the *Open Internet Order of 2010.* This banned the practice of throttling, blocking, and tiered service, as well as classifying ISPs under the heavily regulated *Title II* common carrier. The goal was to create more freedom for citizens by regulating the ISPs.

This was short lived as by 2017 the FCC moved to dismantle *Title II* reforms, and replace it with *Restoring Internet Freedom*; formally approved in 2017, and released in 2018. This meant that FCC and government would step away from actively regulating the ISPs, instead trusting that ISPs would self-regulate with minimal oversight from the Federal Trade Commission (FTC). It's this legal shift that makes the study of net neutrality in the US interesting. In which the state was the main sponsor of security to its citizens, to then transfer to a market driven approach with minimal government involvement. Additionally the ruling interesting is the amount of media coverage and interests from private citizens prior to taking effect. The FCC received 22 million comments on the proposed change, prior to voting. (FCC, 2018a, p. 8). ISPs and business voiced their opinions. Even Burger King created a television ad demonstrating the effects of a tiered system, post net-neutrality, via the example of selling hamburgers at different speeds and rates. (Sottek, 2018). The disruption of net-neutrality wouldn't only affect the US as the internet has no physical boundaries in the

international realm, and can reach any country. Although Europe has their own net-neutrality rules, accessing and interacting with websites, services or data, in the United States may be more difficult and expensive to utilize from outside as well. (Savov, 2017). Furthermore the US can be used as a model for governance, as the legal standard set by the *Open Internet Order* may be a guide for other states responding to their own cyber issues; an international ripple effect.

What we should be asking who should protect the Internet and provide security for its users? Does a business have the capability to serve the interest of the people and their investors? If the government moves away from actively regulating ISPs, can citizens trust ISPs to self-regulate when they have broken regulations in the past?

1.1 Aim of Thesis

This thesis will investigate the judgement of the Federal Communications Commission decision to implement the policy *Declaratory Ruling, Report and Order, and Order: Restoring Internet Freedom.* (2018a). This policy rolls back Obama-era net neutrality measures that were implemented under *Open Internet Order.* My research question asks:

How is the governing of internet access in the United States, as expressed in the new 2018 ruling, affecting citizens' security?

The thesis will be focused on one case, analyzing why the United States decided to dismantle net-neutrality, and the implications of moving away from state regulated security to one that is provided by the market. The theory of Security as Emancipation will be used as a thought tool for analyzing the 2018 decision. The analysis is supported by Kenneth (1991), Laura Shepherds (2013), and Matt McDonald (2012). The goal of using an emancipatory practice is to analyze whether the policy creates more or less security for citizens, by asking 'who are we securing?', 'from what threats?', and 'by what means?' (McDonald, 2012).

The analysis for this thesis is qualitative in nature, utilizing Qualitative Document Analysis as my method, as exemplified by David Altheide and Christopher Schneider (2013). The FCCs *Declaratory Ruling, Report and Order, and Order: Restoring Internet Freedom*, is my main text source, providing insight into the evidence and decision that FCC made. I utilize secondary sources to analyze whether their work had a factual basis for their decision.

1.2 Thesis Outline

In this thesis there are eight chapters in total. The first chapter is an introduction to thesis subject, research question, and outline of the thesis. Chapter two is a discussion on the evolution of net neutrality in the US. Chapter three is a literature review of works that cover the subject of international relations and cyber. Chapter four is the theoretical framework that the analysis derives from. Chapter five pertains to the method and research design of the thesis. Chapter six analyzes information that is used in the FCC case study. Chapter seven discusses US governance as a regulatory state. Chapter eight provides a conclusion to the study.

2. Net Neutrality in the USA

Net neutrality, or network neutrality, can be defined as "…a principle that asserts that governments and Internet service providers should not place restrictions on consumers' access to networks participating in the Internet. In general, net neutrality prevents restrictions on content, platforms, sites and equipment, and modes of communication." (Techopedia, 2018e). In practice this means that all data sent and received on the network will be treated the same regardless of its content, as well as preventing ISPs from preferring specific sites or content. Not only does net neutrality relate to how humans access and operate within the internet, net neutrality also has a direct effect on commercial interests. According to Wired, "Net neutrality advocates have long argued that keeping the Internet an open playing field is crucial for innovation. If broadband providers pick favorites online, new companies and technologies might never have the chance to grow." (Finley, 2018). It's for this reason the FCC pursued net neutrality policies in 2009, as a way to provide security to citizens or at least regulate consumer welfare. "…market forces alone are unlikely to ensure that broadband Internet access service providers will discriminate in socially efficient ways and that, absent regulation, such discrimination is likely to change fundamentally the nature of the Internet, reduce competition, and hinder innovation and growth." (FCC, 2009, p. 28). However for all of the efforts in creating security, Becker, Carlton, and Sider (2010) noted that this regulated security becomes problematic to service providers. "Net neutrality, however, is properly considered a form of price regulation because it limits the form of pricing that can be practiced. Such regulations thus limit a broadband provider's revenue opportunities and its ability to differentiate itself from competitors, and thereby stifle incentives to invest and innovate." (Becker, Carlton, and Sider, 2010, p. 513). This is important to note as in the United States the infrastructure and service of the internet is not a

public good, rather it is reliant upon private companies to provide this support. The operations of these companies are ultimately based on the premise of profit margin, as they must keep their shareholders happy.

If we look at the United States internet services from a historical perspective, we can understand why the government implemented net neutrality principles in the first place. The FCC was created under the *Communications Act of 1934*, providing regulation and equality of service to all US citizens "…without discrimination on the basis of race, color, religion, national origin, or sex, a rapid, efficient, Nation-wide, and world-wide wire and radio communication service…" (47 U.S.C. § 151). This was achieved by creating Title II reforms where service pricing would be regulated and discriminatory practices broken. Companies like the American Telephone and Telegram Company, AT&T, would be regulated as a natural monopoly with oversight of their service, pricing, and to allow smaller operators to use their infrastructure. (Bettilyon, 2017). By 1984, AT&T was forced under antitrust laws to divest the Bell Telephone system into regional carriers in hope of creating more competition. (Ibid). Due to the constraints of operation, these smaller carriers placed less emphasis on the upgrade of the infrastructure, and were not allowed into the cable television and internet services markets. (Brotman, 2016). This changed later under the *Telecommunications Act of 1996,* allowing companies to expand into broadband services. Despite these efforts to create competition, by 2001 Verizon, SBC, BellSouth, and Qwest were servicing 95% of the US population. (Ibid). Furthermore this new Act designated broadband services as a Title I information service as they utilize the existing infrastructure to transmit data from the internet, whereas DSL services remained under Title II as they transmitted data via telephone; effectively allowing broadband providers to operate as they wish. (Bettilyon, 2017). Effectively the light-touch regulations under Title I allowed for ISPs to infringe upon customers access to the internet with minimal preventative oversight. Clear examples of this was found when Verizon throttled access to Netflix and YouTube while their streaming platform, Verizon go90, faced no data capping. (Brodkin, 2017a). Similarly the throttling of peer-to-peer sites like BitTorrent was conducted by Comcast. (Mitchell, 2017). These instances may be considered an inconvenience to the user, a sign of business malpractice, but we should understand that this is part of the greater issue of access.

In 1990, about 1% of the US population was using the internet. (World Bank, 2018). By 2018, the number of non-internet users was estimated at 11% of the US population. (Anderson, Perrin, and Jiang, 2018). Specifically 19% of those individuals cited cost of access as the main attributor. The FCC even estimated that 39% of rural Americans, 23

million people, didn't have access to broadband internet at all. (Malone, 2017). The FCC considers a broadband service as one that provides a minimum connection speed of 25 mbps of download and 3 mbps of upload. (Coldewey, 2018). At those speeds a user would have uninterrupted access to internet applications. In rural places not only is there a difference between services, but the pricing as well. "For around $30 a month, New York City internet providers offer basic packages of 100 Mbps service. As an example, in Saguache County, such a connection is rare; if a household wants a download speed of 12 Mbps with an upload speed of 2 Mbps, they can expect to pay a whopping $90." (Malone, 2017). Having fair and quality access becomes more pressing as our daily lives become more dependent on access to the internet. Even if there is access to the internet the quality is stratified with the possibility of exclusionary practices. Of the actions by ISPs to hinder customer productivity and physical access to the internet, this caused the FCC to step in and take action to provide the necessary security to protect citizens. In 2010 the FCC implemented net neutrality rules under the *Open Internet Order* stating ISPs would stop throttling, blocking, or paid prioritization of internet services, and prevents ISPs from unbundling last mile services. (Kastrenakes, 2015). The FCC went one step further when in 2015 they reclassified ISPs as a Title II common carrier, which gives the FCC the oversight power to prevent practices that hurt US citizens. Despite these measures, the FCC overturned net neutrality under the *Restoring Internet Freedom of 2017.* In a 3-2 decision the FCC repealed Obama era net neutrality rules, re-instated light-touch regulations, transferring oversight to the FTC, and reclassify ISPs as an information service. (FCC, 2018a, p. 2). The thought is that less regulation would drive more competition, and that ISPs would be more incentivized by customers based on economic factors. However deregulation has led to the market with less competition in the past, including inequality in terms of access and treatment of data. What *Restoring Internet Freedom* represents is the governance of the internet in the United States being legally transitioned to a market regulated system, with limited government involvement or oversight, and removes the social dimensions built into how we regulate internet access.

From an outside perspective, could be seen as an issue related to US businesses, however this has far reaching implications for non-US citizens. According to the ITU, they estimate that 51.2% of the world population, 3.9 billion people, will be using the Internet by the end of 2018. (International Telecommunication Union, 2018). To access a website a user is routed through one of many root servers that connects them to the correct location. They are categorized under 13 main servers and share 929 physical locations across the globe for redundancy issues; over 200 of these servers are located in the US. (Root-servers.org, 2018).

In countries like Norway and the European Union, they have their own net neutrality or open internet policies. (Norwegian Communications Authority, 2017). However the data they send or receive via the US may not be treated equally as that of the originating country. This means that they may be susceptible to throttling or deep packet inspection of peer-to-peer files. Essentially the deregulation of net neutrality in the US has far reaching implications, especially when other developing countries look to countries like the US as an example for developing their own laws around regulating the internet. (Savov, 2018).

3. Literature Review

3.1 Defining Cyberspace and Cybersecurity

Cyberspace has become an increasingly larger part of our lives, helping to enhance the human existence. The Internet has allowed us to communicate with others more easily, stay informed about events and trends, access information for knowledge, manage our health and daily lives, to enriching our lives with entertainment as well. (Anderson and Rainie, 2018). The utilization of the internet in healthcare services allows for greater access to patients records and virtual appointments, while the farming industry has benefited from better monitoring systems of water usage and crop yield, and cities are able to observer pollution and manage city services more easily. (Kranz, 2018). Despite the opportunities, cyberspace has vulnerabilities in the system that threat actors aim to exploit. Threat actors, or malicious actors, are defined as "…cyberterrorists, hacktivists, state-sponsored actors, and cybercriminals". (Ablon, 2018, p. 2). Threat actors may implement malware tools to infect devices or disrupt networks, implement attacks within the physical and digital worlds, as well as attempt to gain access to sensitive Personally Identifying Information (PII) or other secretive data. (Ibid). Access to cyberspace may also be hindered by the operation of an Internet Service Provider (ISP) via physical limitations of infrastructure or a deliberate alteration of network connections, as well as the cyber policies set by a government. In the wake of such issue, cybersecurity as a field has risen to combat or mitigate these problems.

Cybersecurity is a burgeoning field, however it wasn't until 2010 the International Telecommunications Union (ITU), an agency under the United Nations, described cybersecurity as "…the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets…" (Radu, 2013, p. 12-13). Even with a definition of cybersecurity, Roxana Radu noted that states are left to find a balance between security and freedom. States that practice a

liberalized internet practice provide greater freedoms to their citizens at the risk of security; whereas a state imposing stricter access, in the form of filtering and surveilling data, may find more security at the cost of freedom. (Radu, 2013, p. 14). In the United States, previous security policies have allowed citizens to freely navigate and use the internet. However previous the light-touch regulations essentially allowed ISPs to determine what was best for their business by controlling access and content, as well as physical infrastructure. (Bettilyon, 2017).

Cybersecurity also directly relate to the "…technologies, processes, and policies that help to prevent or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology (IT) by a malevolent actor." (Clark et al, 2014, p. 1). When we engage in the conversation of cybersecurity we must understand the relation to the cyberspace domain. Cyberspace operates within three arenas: a digital arena, a physical component of infrastructure or technological hardware, and digital information and software. (Clark, Berson and Lin, 2014, p. 8). In the case of *Restoring Internet Freedom*, cyberspace would include the ISPs operation of transferring data between user and end user, as well as the physical infrastructure developed by ISPs to support the internet. The 2018 order would be considered a form of cybersecurity by the ITU as it is a policy to set guidelines for how ISPs should operate and how they will create more security for citizens. We find that it discusses the change of ISPs from a telecommunications service to that of an information service, allowing ISPs to determine how best to facilitate digital access of internet for users. (FCC, 2018a, p. 2-3). The policy also hopes that a light-touch regulation would push ISPs to maintain and develop infrastructure of the network in order to attract more customer; with security being linked to physical access. (Ibid).

Ronald Deibert (cited by Hansen and Nissenbaum 2009) argued cybersecurity constituted as "…four separate discourses with distinct referent objects, threats, policy options, and world orders: national security, state security…, private security, and network security…" (Hansen and Nissenbaum, 2009, p. 1163). However, Hansen and Nissenbaum see the field of cybersecurity as being less fragmented due to the interconnectivity of referent objects. "Particularly crucial in the case of cyber security is the linkage between 'networks' and 'individual' and human collective referent objects." (Ibid). In my case the referent object would be citizens and the concern equal access, and treatment of data, to the internet. In the case of the *Restoring Internet Freedom* the government is stating that security is more achievable under less regulations and that the market would be a better guarantor of that

security; whereas the opposition believe that the citizen are more secured under government policies like net neutrality that guarantee needed security.

International relations scholars have widened the study of cybersecurity by including the concepts of "power, sovereignty, global governance, and securitization." (Maurer and Ebert, 2017). These concepts help to evaluate the subject of cyber from a wider array of threats, including "…cyberwarfare, cyberconflict, cyberterrorism, cybercrime, and cyberespionage as well as cybercontent, while narrower conceptualizations focus on the more technical aspects relating to network and computer security." (Ibid). When we engage in a security discourse, we must be aware that without proper vetting or analysis of a security topic, it may be hyper inflate the actual perceived object at risk. "…security discourse has served to legitimize actions within the policy because the term 'security'…gives priority to the theme, thus resulting in its application on a security agenda." (Garcia and Palhares, 2013, p. 276). As *Restoring Internet Freedom* is relatively new, opponents fear will allow for ISPs to dictate broadband service, effectively claiming a security concern without solid evidence. Contrary to popular belief, ISPs have asserted that discriminatory practices would not be used under this new order, backed by company pledges. (Rizzo, 2018).

What we should remember is that cyberspace is an arena and tool that helps to conduct our business and daily lives. With that we are susceptible to threat actors that may wish to alter that connection. However cybersecurity is the operation and tools that are utilized to reduce those risks. Not only does cybersecurity operate in a digital field, but relates to the protection of physical infrastructure.

3.2 Cyberspace and International Relations

In field of international relations Lucas Kello notes that there is a skepticism amongst scholars regarding cybersecurity, which may hinder the ability to academically engage the topic. He sees the main issue is too much and too little data available, and the classification of the of cyber activities and issues. "The first concerns the paucity of cases available to propose, test, and refine theoretical claims on cyber phenomena." (Kello, 2013, p. 9). Even with reported attacks on private and public entities, insufficient data and lack of metrics prevent in-depth analysis. The secrecy of cyber events and programs creates skepticism, and difficulties in producing data. Creating the belied that technical qualities of cyber related events, tools, and study play a role in how well a scholar can perceive the subject. "…you

really need to know a great deal about computer networks, software, encryption, etc. to know how serious the danger might be." (Kello, 2013, p. 10).

In Robert Reardon and Nazli Choucri (2012) they reviewing articles on cyberspace and information technology that appeared in 26 major scholarly international relations and political science journals from 2001-2010. Articles were greater than four pages, and "…focused largely on issues related to cyberspace, information and communication technologies (ICTs), the Internet and Internet-based social media, or the 'information revolution'…concentrated largely on international issues. (Reardon and Choucri, 2012, p. 3). They reviewed a total of 49 articles and categorized them into five areas of study "…global civil society, the governance of cyberspace, economic development, the effects of cyberspace on authoritarian regimes, and security." (Reardon and Choucri, 2012, p. 4). Of these articles they found academic and policy literatures shared a greater focus on cyber security, while academic literature covered topics within governance and the effect on global civil society. (Ibid).

Reardon and Choucri point out that the five issue areas "…suggests that there is broad agreement among the international relations community, both academic and policy-oriented, about what the most important debates are over cyberspace." (2012, p. 25). These articles were seen to have the themes of defining cyber-related phenomena and the conceptual framework for analysis, the transformative effect of cyberspace on international politics, and the relationship between international politics and technological change. (Ibid). Although they were able to identify the key themes within cyber, they found that categorizing the studied articles into the five issue areas was problematic as it "…illustrates how little work has been done, at least in the major journals, on conceptual themes and theoretical puzzles related to cyberspace that connect these five issue areas." (Reardon and Choucri, 2012, p. 25). This is why when conducting data collection and research on cybersecurity in relation to my subject it was difficult to find academic material to help explain the intricacies of my study.

It's important to understand that cybersecurity has often been portrayed as an element of a militarized study by academics, politicians, and media. News media like Forbes Magazine may publish articles by O'Flaherty (2018), detailing past attacks by foreign powers and their possible motives and tools. While politicians like Senators Mike Rounds, Dan Sullivan, and Martin Heinrich, previous U.S. House Armed Services Committee members, portray the issue of cybersecurity as a defensive national security matter as the US has been a repeat target. (Mahtesian and Shafer, 2018). However the idea that cyber fits within the

context of warfare doesn't fit as warfare has an element of physicality and violence perpetrated by an act of force on an opponent. (Rid, 2011, p. 7-8). Rid does agree that an attack via cyber means could be an act of war, but the process of conducting operations and outcome differ from traditional ideations of war. Cyberwarfare may still impact economies, physical infrastructure, communications, and possibly inflict casualties. However he notes where it deviates away from traditional warfare is that cyber activities aim to primarily disrupt systems through a specific set of action. (Rid, 2011, p. 9). Instead, cyberattacks generally fall into the areas of sabotage, espionage, and subversion, which can considered as a military or political tool. (Rid, 2011, p. 16). However John Stone, senior lecturer at King's College London, disagrees with Rids' understanding of cyber in relation to war. "…war demands no necessary causal connection between what are really three distinct phenomena…all war involves force, but force does not necessarily imply violence – particularly if violence implies lethality." (Stone, 2012, p. 103). Technology may be a medium to conduct malicious activity, it can also be a catalyst or force to drive the larger theater of war. In terms of my case study, private actors like ISPs may not intend to harm customers, however they have historically hindered customers by disrupting service or blocking websites, and denied the expansion of infrastructure. (Bettilyon, 2017). This could be categorized as a form of sabotage.

Reardon and Choucri agree for the most part with Rids' assessment. They found the scholars who wrote on security "…discuss a wide variety of phenomena – so wide, in fact, that it begs the question of exactly what is meant when the authors use terms such as 'cyber conflict,' 'cyber security,' or 'cyber warfare.'" (Reardon and Choucri, 2012, p. 19-20). Scholars like Goldman and Newmyer see cyber as a new tool with military capabilities and applications, while scholars Kohlman and Brachman also note non-state actors may use cyber tools to disrupt states. (Reardon and Choucri, 2012, p. 21-24). Overall Reardon and Choucri found a majority of the authors speaking on cybersecurity transformed it from "…a term originally reserved for the technical integrity of networks…" to "…a matter of national security and high politics." (2012, p. 24). We can then surmise that the translating of cyber issues from a non-physical digital terrain to the physical world, allows for a larger audience to participate in the subject; by using terms of militaristic actions or threats audiences have a greater frame of reference. However this is problematic as it deviates from what actually constitutes cybersecurity and cyber threats, especially when the ideation of those threats may be hyper-inflated due to the referent object.

Reardon and Choucri noted the frame of reference in relation to the cybersecurity of a state can suffer from being too inclusive in terms of a security subjects. The study of cybersecurity is then cast into two areas of interest. "…there is a discussion about the nature of the threat and potential means to address it. On another, there is a meta-discussion about the ontology and epistemology of cyber security, and the evolution of the concept." (Reardon and Choucri, 2012, p. 20). If the study of cybersecurity then becomes alarmist or reactionary to a threat it becomes more difficult to actively assess the subject from an unbiased viewpoint, especially if there are special interests or organizations involved that benefit from this attention. As an example, Richard A. Clarke was an advisor on developing and implementing United States cyber security policies under Presidents Bill Clinton and George W. Bush, and served on President Obama's Review Group on Intelligence and Technology. (Future State Podcast, 2018). He went on to write *Cyber War* in 2010, exposing the threat of cyber to US national security. Although the literature was insightful and his knowledge invaluable, it should be taken with a grain of salt considering he is the Chairman and CEO of Good Harbor Security Risk Management LLC, a company that provides cybersecurity services on risk analysis and solutions among other things. (Good Harbor Cyber Security Risk Management, 2018).

How we talk about cyber then relates to a discursive engagement, which can determine the traction that a subject receives. According to David Clark (cited by Reardon and Choucri 2012), "…the terms 'attack,' 'war,' 'threat,' and 'security' are used ambiguously, and often refer to activities that are not generally viewed as acts of war or threats to national security." (Reardon and Choucri, 2012, p. 24). Thomas Rid doesn't deny that cyber risks and challenges are on the rise, however when cyber threats are mislabeled it becomes problematic especially when labeled as an act of war. (Rid, 2011, p. 15). In my study, the understanding of the FCCs motives was met with minimal or misinformation on the effects of the possible new ruling, but garnered a lot of anger overtime. When comedian John Oliver discussed a segment on the FCC directing the audience to voice their opinion, the FCCs public comment system received 22 million comments within a span of two days, crashing the website. (Kelly, 2018a). With comments often insufficient to be registered as a valid complaint.

This would mean that the study of security is more of a self-referential exercise. Where a threat becomes of 'security importance' in relation to: political importance, states history, geographical and structural importance, and reaction by others internationally and domestically. (Buzan and Hansen, 2016, p. 34). Additionally, "For security speech acts to be

successful, they also need to convince their relevant audiences." (Ibid). This becomes problematic when there are individuals or organizations that benefit from overinflating the importance of the subject, as it makes it more difficult to accurately assessing the issue from a policy standpoint. Kello notes that scholars may see that cyber related attacks and weapons are generally relegated military affairs than other appropriate policy venues. Despite this prevalent thinking "…the claim of threat inflation makes a direct appeal to the preconceptions of security scholars, arguing that threats that appear to lack an overtly physical character or that do not rise to the level of interstate violence are intellectually uninteresting." (Kello, 2013, p. 11). Similarly we could say that by focusing *Restoring Internet Freedom* in terms of business and legal aspect can then lead security scholars to believe that it's not of importance to study. Whereas a policy speaks on the state's ability, or desire, to guarantee security of citizens to the right of equal internet access.

Although the study of cyber is portrayed as an area of misunderstanding and limitations due to technological attributes, cyber does have a place within international relations, as "…integrating cyber realities into the international security studies agenda is necessary both for developing effective policies and for enhancing the field's intellectual progress." (Kello, 2013, p. 8). Yet, as Kello mentioned earlier the problem is that cyber is often avoided by scholars due to the perception that cyber is difficult to master; and that cyber has merit when it breaks into the physical realm of security. (Kello, 2013, p. 11). However, he argues that these skeptics are wrong in that threat inflation can be used to assess the scale of danger, nullifying the idea that cyber issues are incomprehensible." (Ibid). If scholars are then able to assess cyber issues on a continual basis we can then begin to bridge the gap between the scholarly and policy.

Ultimately the perception that cyber needs technical expertise is inaccurate cyber shouldn't come with a high degree of learning, instead "…only the minimum degree of technical acuity is needed, which reveals the scope of maneuver in the cyber domain." (Kello, 2013, p. 16). However, the knowledge of cyber does not mean scholars are to become experts, instead they should rely on technical experts to provide the assessment of the deeper intricacies of cyber. "Certain aspects of the cyber issue, such as the analysis of code, belong to the computer specialist; others require the expertise of researchers versed in the contests of international anarchy." (Ibid). From my own perspective, going into my research I had a basic understanding of cyber. However as I began to read more material I found it easy to comprehend the subject. When I had issues I was able to find my answer from a quick browser search or query to a specific Reddit group for guidance to a proper source.

Kello sees the analysis of cyber similarly to methods within international security studies. The subject should be manageable, identify the features and phenomena of the technology or event, codify collected data collected after a cyber event, search determining factors of the event, and establish points of reference to explain the event. (Kello, 2013, p. 17). This framework has similar qualities to other studies, this framework asks for scholars to specifically identify the cyber issue prior to data collection and analysis, developing a history for other cyber scholars to utilize. The theory that then is created from these studies can be utilized in crafting policy, which then helps to inform if the theory is correct. "The need to establish a field of cyber studies rests on the premise that policy succeeds or fails based on the correctness of the theory it presupposes." (Kello, 2013, p. 14).

3.3 Cybersecurity Policy and Global Governance of the Internet

The application of cyber in the US has conflicting interests and equities as a point of contention to policymaking. "As a nation, we want better cybersecurity, yes, but we also want a private sector that innovates rapidly, the convenience of not having to worry about cybersecurity, and the right to no diminution in our civil liberties." (Clark and Berson, 2014, p. 2). Not only does policymaking suffer due to political demands and special interests, cyber policies also suffer due to the preconceived ideas on how best to attend to cyber matters. "Generally, national leaders turn to past policies – based on past realities - when responding to new challenges. In some arenas, this can be a wise practice, and one supported by institutional and bureaucratic logic, but there are no precedents for cyberspace as a domain of international interaction." (Choucri and Goldsmith, 2012, p. 76). When it comes to the realities of cyber policies for states, the arena is always evolving, to rely on old methods or ideas places you at risk. In terms of the FCC decision to return to light-touch regulations, although it was championed by conservatives as a win for businesses, we can see the negative impacts it had on access and competition as noted by Bettilyon (2017) and Malone (2017).

Despite these issues for cyber policymakers, Kello believes that this proves an opportunity for international relations scholars to provide insight on cybersecurity. As mentioned before in Kellos' framework for studying cyber, scholars may be able to identify cyber issues in relation to a theory, and have a greater impact on policy making by providing accurate tools and theories to cyber trends. This becomes important especially when policymakers lack the proficiency or knowledge to address cyber issues. However we must also keep in mind that scholars may have to compete with others vying for the interest of policymakers. "The policy challenge is to render the toolkit of policy responses more

consistent with the complexities of cyber realities. So far, cyberspace has been an open arena. But this is changing. In the United States, lawmakers are struggling with how to manage competing interests..." (Choucri and Goldsmith, 2012, p. 74).

Although the Internet was designed to be open, Joseph Nye notes that a level of governance will naturally occur. "By its very nature, the interconnected cyber domain requires a degree of cooperation and governments becoming aware of this situation…cyberspace has a number of areas of private and public governance." (Nye, 2011, p. 30). Nye notes that a problem with current governance solutions is that it's always answering to a problem, where "…national governments try to manage problems of security…within national legal frameworks, though the technological volatility of the cyber domain means that laws and regulations are always chasing a moving target." (Nye, 2010, p. 15). The FCC and US policy towards internet security of its citizen's show that governance is a balance to achieve. Reardon and Choucri noted in their study that the subject of governance has garnered a lot of attention in cybersecurity. According to the Working Group on Internet Governance, they define Internet governance as the "…the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." (de Bossey, 2005, p. 4). Specifically relating to cyber, governance tends to analyze a stakeholder's ability to influence and determine the governance structure of the cyberspace, specifically the "…technical standards, regulations, and institutions that determine the structure of cyberspace is the central issue in the governance of cyberspace." (Reardon and Choucri, 2012, p. 11).

However it's found that cyber governance decisions tend to be dominated primarily by powerful state, and that a decision on governance by one state, or a subsect of states, can determine the direction of cyber governance for all. As an example the Convention on Cybercrime, or Budapest Convention, led by the Council of Europe had a specific focus on copyright infringement, violations of network security, and Internet espionage, and tried to foster international cooperation and prosecutorial procedures. (Choucri and Goldsmith, 2012, p. 3). As the Council of Europe is a large governing body they are able to sway international standards for how to combat the issues that were focused on, creating an order that best fits their needs. Members of the convention all agreed upon the ability for other states to gain access to their cyber networks, in relation to tracking cybercrime. "Some countries, most notably Russia, have objected to this provision on the basis that it 'might damage the sovereignty and security of member countries and their citizens' rights'." (Clough, 2014, p.

719). Russia being a member of the Council of Europe is effectively not able to change the treaty due to all other members agreeing to the treaty. Additionally Russia wishes to introduce their own cybercrime legislation in the United Nations, with help of China and the Shanghai Cooperation Organization. (Ignatius, 2018). Although they are looking to get support from developing nations, Russia will not get support from member of the Council of Europe as they already have an agreement, thus the Russian endeavor is nullified through this lack of support.

Reardon and Choucri also found that the stronger states may opt to create their own governance structure, or develop agreements with other specific states, when not in agreement with international governance policies. The International Safe Harbor Privacy Principles of 2000 to 2015 by the European Union (EU) created guidelines for international data protection, specifically the protection and storage of EU customer data from being distributed to outside 3rd party sources. To circumvent this, the EU and United States created the joint Safe Harbor agreement outside of EU protection regulations, allowing for companies and organizations to transfer data with the expectation that personal data would be handled correctly. (Reardon and Choucri, 2012, p. 12) Additionally cyber governance is not solely dependent on states and power dynamics, as non-state actors have the ability to play a role as well. "Non-governmental and private actors serve primarily as agenda-setters. … (though) non-state actors can still leverage their technical expertise to influence outcomes, and leaves open the question of how great a role other actors can play." (Ibid). By including technical experts and organizations that devote their work to cyber governance, non-state actors can help to develop draw out the essence of the issue and pursue a correct course of action; especially when other actors lack knowledge. In *Restoring Internet Freedom*, we saw the inclusion of non-profits and think tanks in the decision process as they could provide expertise and analysis that eh FCC may not be able to conduct or comprehend.

Amongst the studied governance articles, Reardon and Choucri noted a focus on the relation to inclusivity and openness. "Nearly all authors favor a more inclusive and democratic arrangement for cyberspace governance that better represents the diversity of stakeholders. Outside of the liberal West, few stakeholders are willing to support continuing the Internet's existing architecture." (Reardon and Choucri, 2012, p. 14). Such divide was seen within the Internet Governance Forum (IGF) during the World Summit on the Information Society (WSIS) in 2006. According to the Council on Foreign Relations (CFR), states from across the political spectrum, private sector and civil society groups, were able to gather and equally participate in policy discussions. (Masters, 2014). Participating states at

the IGF included liberal leaning ideologies, such as the Council of Europe and the Government of Quebec, as well as states that share authoritarian characteristics, such as Russia and Egypt. (Internet Governance Forum Secretariat, 2006, p. 17). One particular subject discussed at the IGF regarded the unilateral oversight of the Internet Corporation for Assigned Names and Numbers (ICANN) by the United States from 2006-2016. In 2006 the United States Department of Commerce (DoC) renewed a Memorandum of Understanding with ICANN to retain control of the Internet Assigned Numbers Association (IANA), effectively giving the United States government partial control of ICANN and the A Root Server. (Benedek, Bauer and Kettemann, 2008, p. 16-17). The IANA provides oversight of Internet Protocol (IP) address and Autonomous System (AS) number registries, standardization of media file types, as well as management of the DNS Root Servers. (IANA, 2018). The function of the DNS root servers is to allocate the correct IP addresses to the domain name, which is divided between Top Level Domain (TLD) and Second Level Domain (SLD). TLDs are what ends after the site address name, such as .com, .org, or two letter country codes like .no or .fr; while SLDs refer to the unique site name prior to the TLD, such as Google in google.com. (OECD, 2006, p. 4). The OECD noted that some TLDs have specific requirements to be met prior to being registered, while some states may be have more liberalized with less requirements. In 2005, liberalized TLDs (ex: China, Brazil and India) saw an increase of registrants by 36% in 2005 compared to a 9% increase under OECD states. (OECD, 2006, p. 5). Although a liberalized TLD may have increased cost and administrative processes, its fond that it curbs cyber-squatting, online fraud and intellectual property violation, and assures individuals they are dealing with legitimate websites. (Ibid). Additionally the Governmental Advisory Committee (GAC), made of 100+ states, advises the Board of Directors of ICANN. There is an overall low turn-out at meetings, but a consistent presence of the liberal leaning OECD member states which provides a dominantly liberalized point of view. (Benedek, Bauer and Kettemann, 2008, p. 16-17). For example in the *GAC Principles Regarding New gTLDs* (2007), it was suggested to ICANN that new generic TLDs should respect “The provisions of the Universal Declaration of Human Rights.” (Governmental Advisory Committee, 2007, p. 2). Some states have expressed concern for the liberal perspectives of ICANN. At UN-sponsored World Conference on International Telecommunications of 2012, it was reported that Russia, China, Saudi Arabia, Algeria, and Sudan proposed that, “Member States shall have the sovereign right to establish and implement public policy, including international policy, on matters of Internet governance." (Masters, 2014). The United States took issue, stating that “…Internet policy

must be multistakeholder-driven. Internet policy should not be determined by member states, but by citizens, communities, and broader society." (Ibid). Additionally, in 2017, Russian President Vladimir Putin called for development of an independent root server from ICANN and DNS, utilized by BRICS member states, Brazil, Russia, India, China, and South Africa, by August 2018. (Goncharenko, 2018). The Russian Security Council reasoned "…the 'dominance of the US and a few EU states concerning Internet regulation' which Russia sees as a 'serious danger' to its safety…Having its own root servers would make Russia independent of monitors like the International Corporation for Assigned Names and Numbers (ICANN) and protect the country in the event of "outages or deliberate interference." (Ibid). What this demonstrates is that the larger voice does have control of the cyber agenda, and that other states must follow along to the set agenda, or be willing to not participate and still face the legal standards set by state.

Although policy discussions on an international scale may have their issues, this venue does allow for greater participation and understanding of the cyber dilemma. "Farrell provides the important insight that persuasion can be an effective mechanism for shared governance, and a tool for reconciling fundamental differences in values. If cyberspace indeed promises to have a progressive transformative effect on international politics, or can do so under certain conditions – a claim that very much remains open to question – then the governing institutions that shape cyberspace's architecture, and in turn its social political effects, will be critical." (Reardon and Choucri, 2012, p. 14).

4. Theoretical Framework

4.1 Critical Security Studies

For the last half of the 20th century, security has been predominantly controlled by a realist discourse, with an emphasis on military threats and the protection of the state and its status quo. (Booth, 1991, p. 318). For realist this is more than enough to determine state security. In comparison, post-structuralism questions the idea of 'who' is being represented within security, while constructivists ask the identity of the referent object. This convergence of identity and representation is investigated further within the area of Critical Security Studies (CSS). CSS notes that humans are, and should be, placed above the state in order of importance, and threats to security should be expanded to include non-traditional threats as well. Booth reasons for widening the security debate as not all threats to humanity are of militarized action. These threats can be "…from other challenges, such as economic collapse, political oppression, scarcity, overpopulation, ethnic rivalry, the destruction of nature,

terrorism, crime and disease." (Booth, 1991, p. 318). This reasons that the individual should be the ultimate referent object, as states are unreliable and diverse to provide security. (Buzan and Hansen, 2009, p. 206). In other words, although the security of a State is of importance, the security of citizens can determines the overall security of the State, lending legitimacy to a state. If we look at this from the perspective of cybersecurity, we should be asking if the policies in place benefit everyone, or if they protect only the states interests. As the average security dilemma for individuals go beyond that of threats to the state, we can see a CSS perspective widens the threat base for the insecurities that individuals might face, such as the cybersecurity needs of a state.

4.2 Security as Discourse

When analyzing the securitization of a referent object, we should ask "…whose security; from what threats; through what actors; by what means?" (McDonald, 2012). This would mean that a states security is a social construction that is created by society, in that the context of that threat is evaluated through different political communities, analyzing the content of the threat. (Ibid). To understand security as a construct of society we must understand how and why the referent object requires security. However, the process of identifying the issue for securitization can be inconsistent by the values and ideology that accompany political parties or affiliation. Within a political system you can have many parties or groups that require certain measures of security and how they would like it achieved. The United States is no exception, the dominant two party system may share opposite opinions on issues and become partisan or zero-sum oriented in action, rather than finding a compromise that is mutually beneficial to all. Even the FCC as an independent agency is subject to the partisan politics.

"Central in all critical constructivist accounts of security is the intersection between security, identity and representation." (McDonald, 2012). For a referent object to become securitized an identity has to be developed in the form of language or societal context, though language and context aren't effective unless it resonates within a society. This means that resonance is directly related to representation, which legitimizes a claim for a referent object to be securitized. As with my example in the United States, individuals who feel that a repeal of net-neutrality undermines the security and freedom they have on the Internet can claim that all individuals across the United States, especially when a democratized society shares a common value of freedom. Similarly, McDonald points out that to claim something needs to

be secured, it first has to have legitimacy. A politicians ability to declare something to be of a security concern is limited if it doesn't have clear implications as to whom they are trying to secure. The role of a politician is to represent their citizens as a collective, which is to act in the best interest of their constituents by listening to the needs and of the citizens. Similarly, an individual's ability to become a politician is based on support, which means that citizens have the ability remove leaders from power if they aren't acting in the best interest of their constituents. However, individuals have to rely upon politicians due the status and capacity to develop or dismantle security interests more easily, as well as developing common opinions with other leaders. "While some claims might genuinely be more convincing, compelling and ultimately resonant than others, the question of the position of the speaker, their material capacity to speak and have their voice heard, and even the capacity to translate representation into action is all central to the discourse of security that comes to 'win out' in any political context." (McDonald, 2012). If a state acts on the behest of the people, it is easy to understand how a law is created because we can see how it had support from citizens. Here lies the issue of the FCC decision: was the choice made to directly protect citizens or was the interest in having market driven security with minimal government interference.

Again, a realist approach to security would consider the state as the ultimate referent object for security, or ultimate producer of security. A constructivist approach to security goes beyond this "…acknowledging that any issues can potentially be considered and constructed inter-subjectively as a security issue in a particular context."(McDonald, 2012). To define a security threat as a referent object is, as McDonald suggests, a discursive approach to creating security, with respect to the meaning we give to the referent object and core values. However McDonald warns that this can become an issue as the political actors will be the one to claim what is and isn't a security need, including the level of importance, as well as how the issue is disseminated and concluded. Instead he points out the need for alternative actors to raise issues. "I therefore retain a view that the designation of threat has particular political force and is an important security representation, but suggest the need to broaden our analysis to look at alternative security interventions." Further we should also be concerned not only how security concerns are brought to light, but for whom the security is developed. The way the FCC phrases the need to repeal net neutrality focuses less on the needs of citizens, and more on the prospects for business innovation, which could lead to greater human security. Again, we ask who they really intend to protect.

4.3 Security As Emancipation

Part of the issue of applying security to society, as Booth pointed out is that it can become harder for outsiders to influence a debate or action, as he found in the nuclear deterrence debate. “Over the years nuclear deterrence theory became increasingly esoteric, rococo and irrelevant. It led to a somewhat closed world, protected from politics and morality by 'mindguards' and 'nukespeak', and a belief in timeless success.” (Booth, 1991, p. 322). By utilizing an emancipatory practice as a tool for analysis, this may be able to avoid stagnation and widen the security debate. Before utilizing an emancipatory tool for security, we need a definition of emancipation as a concept.

McDonald assessed that when emancipation was first conceptualized within the Frankfurt School, it was primarily based on the idea of enslavement to a system, “…freeing the most vulnerable that escaped from the potentially limiting focus on the proletariat as agents of change or exclusively economic sources of oppression or inequality.” (McDonald, 2012). The issue with this definition is that it describes emancipation through a specific aspect, and less about political implications; additionally it doesn’t quite explain the overarching goal of emancipation. Over time the meaning of emancipation evolved and came to be understood as “…the freeing of individuals from arbitrary structures that prevent them from living as they would wish.” (McDonald, 2012). This definition broadens the context of emancipation in terms of what can be a referent object, who can be considered an affected individual, as well as an avenue for political context, but leaves little interpretation as it creates the conversation for change.

Building upon the Frankfurt school, the theorists at the University of Wales Aberystwyth, or the Welsh School, considered emancipation as more concerned with the broadening of security from a state and military security observation, to asking for whom the state is ultimately providing security. According to Booth “States, however, should be treated as means and not ends. It is on the position of the state where the conception of security as a process of emancipation.” (1991, p. 319). McDonald agrees on this point as well, saying “…states could indeed be viewed as *possible* agents for security: means for advancing the wellbeing of their own citizens.” (McDonald, 2012). One critique McDonald has of the Welsh school of thought is that they are particularly more interested in the individual than larger groups or communities. I do see his point; however acting to create emancipatory change for one person could be representative of a larger group if they share the same dilemma. In the context of cybersecurity, the FCC only made efforts to change the system when they saw a perceived failure of protecting a large population of citizens prior to the

Open Internet Order, and similarly under *Restoring Internet Freedom.* However, McDonald points out that the Welsh School, specifically Ken Booth, believes the State can be the agent for change, but doesn't quite define if non-state actors can be one of the same. Richard Wyn Jones argues that academics could provide agency as a non-state actor for emancipatory change. "…the second potential source for understanding emancipation in concrete terms comes into play, namely, the work of those scholars attempting to apply the insights of critical theory to the study of world politics." (Jones, 1999). Academics can participate as a non-state actor due to their credibility, and capacity to develop thoughtful narratives. If it is then possible for academics to fill the role of agency, then we could surmise that citizens or advocacy groups could be an agency for change as well. Although organization like EFF and AEI have their own agenda when speaking with the FCC, they reflect the opinion of individuals. Both parties then are able to gain legitimacy. Additionally, the FCC had an online comment system available for citizens to express their opinion. Although it was less than stellar, the FCC did in a sense offer agency to citizens in a sense.

Although both the Frankfurt School and Welsh School provide their own understanding of emancipation, they both aspire to emancipatory change as a goal, and ask whom should act upon it. Based on their definitions, a state's overall objective is to provide freedom and security for all citizens. Based on my case study, this can be done through the act of accepting or striking legal statutes that hinder the ability. The FCC viewed that the previous net neutrality measures were hindering ISPs from delivering the best possible service, and that the US government should strike down that ruling to create more security. This would mean that the best practice for achieving emancipatory change is through a security discourse as it aims to removes structures of oppression and exclusion. "Whether locating possibilities for emancipation in terms of production or communication, critical theorists have consistently emphasized the central moral imperative of removing arbitrary and oppressive structures." (McDonald, 2012). Despite much of the emancipatory discourse surrounding the idea of the 'other' or disenfranchised individuals, we could apply this to a larger context where individuals or groups lack the ability to affect legal change or have a voice in the process of developing legal change. By adopting net neutrality measures the US was recognizing that individual access to the internet was being oppressed by discriminatory practices, as well excluded due to their physical location.

The basis for critical security discourse asks 'who are we securing?', 'from what threats?', and 'by what means?' (McDonald, 2012). The definition of emancipation and the understanding that security discourse aids in moving the conversation from the margins to the

center, we can start to see how emancipation can lead to change. “Emancipatory change therefore can be defined in terms of steps towards the removal of arbitrary and oppressive structural constraints.” (McDonald, 2012). This ideation of how emancipation can affect change is important to understand as it doesn’t stand to solve an issue, rather helps to develop the process for possible change. Referring back to my topic, the tool of emancipation can then ask if the FCC decision to remove net-neutrality measures happened because they felt the initial measures were oppressive to the citizens of the United States, if not we must then ask for whom did the decision represent. McDonald does mention that there are a few things to be aware of while researching cases of emancipation. We may find the best intentions for emancipatory change can be achieved through outcomes derived from a gradual change and support within the society, such as the grassroots movement and individual state laws supporting same-sex marriage that led to the United States Supreme Court granting equal rights in 2015. “Emancipatory change must be incremental and developed within political communities in order to be sustainable and to bring genuine benefit to those concerned.” (McDonald, 2012). If the issue can’t keep the attention or support of the public, the issue may fail to gain traction to the final resolution. Similarly to develop a law that has little backing makes it harder to gain acceptance, which can lead to other actors challenging the new measures of security. In turn it also shows that a popular opinion within a society can develop discourse that may drive change as well.

Emancipatory discourse can lead to political practice through community building, or by “break(ing) down the barriers between ‘us’ and ‘them’.” (Booth, 1991, p. 324). Otherwise known as ‘process utopian’, its suggested that to make emancipatory change the agent must focus on steps in the process to creating change, rather than focusing on the overall problems of the structure. Due to the nature of the Federal Communications Commission decision, individuals have little recourse in ability to change the original decision. Nevertheless, on the local state level, they have started to create their own net-neutrality laws that go against the FCC decision, which could set a trend amongst other states within the United States. With this approach, you don’t necessarily have to rely upon the state to provide the means for emancipation. “The process Utopian approach is not confined to governments. There is growing scope for non-state actors, such as the 18,000 INGOs which are creating…a ‘global civic culture’.” (Booth, 1991, p. 324-325). Not only is this applicable on an international level, we can apply the same principles on a national level in the United States by an organization that can establish a narrative around an object that needs securing. For example,

the Electronic Frontier Foundation and their agenda for net-neutrality measures to be adopted for greater internet security.

From this we know that the goal of security as emancipation understands individuals should not be hindered by regulations that impede their ability live freely, and if so the state may help to facilitate the process of emancipation. We can start to explore this through discourse in asking who security is made for and from what are we trying to secure. We also know that emancipatory change doesn't have to be dependent on the state to develop the conversation. The final piece to understanding security as emancipation is how this translates from a theoretical stand point to a real world application. Laura Shepherd (2013) lays out how we can use an emancipatory tool for analysis. By Investigating the claims of different actors and their socio-political position, the practice of security should assume a political motive, and that the goal of security should identify the possibility for emancipatory change. (Shepherd, 2013, p. 74). Within my case the can the referent object would be the citizens of the US, and that FCC regards the 2009 and 2015 net neutrality rulings as an infringement upon the security of citizens to conduct their business or have access to the internet. This can be determined by analyzing the net neutrality law and how it might make an individual life more difficult. As well as look at the 2018 ruling and understanding if it delivers more security. The analysts or researchers role is to identify if the new law will provide the ability to create emancipatory measures. In my research it would be to find if the existing or new net-neutrality laws would allow for emancipatory change, beyond what could be provided by net neutrality principles.

4.4 Critique of Security as Emancipation.

Buzan and Hansen note that critics of SAE find that claiming the referent object focus on individual and collective security. "Emancipated individuals are in need of a resolution at the collective level and to envisage this as unproblematically flowing from the individual level leads back to a classical utopian level." (Buzan and Hansen, 2009, p. 207). Additionally an emancipatory practice suffers from a vague description and a lack of metrics. However critical security theorist argue the approach to emancipation has more to do with opening the security debate to a wider audience, which lends the ability to identify threats more easily. (Ibid). With regards to the critique, we need to look back at the originating goal of emancipation as it is a tool to help us analyze if the current security levels are designed to help those that are vulnerable or not. As an analytical tool it's goal isn't as much to create solutions, more so to aid the process in identifying the underlying problems. The FCC was

originally created as an agency to help the US government determine issues within the communications spectrum, thereby widening the security debate. Secondly, despite framing the referent object around individuals we can come to understand that if one individual is negatively affected, in all likeliness they aren't the only individual. It might start with the individual, we may can extrapolate the underlying issue to the effects on a larger community.

4.5 Multistakeholder Governance Model: A Framework for Security

Even though we may understand that the goals and potentials of SAE as a tool for developing the conversation of security, a tool is only useful if it can be put to work. This is why we must apply SAE to a governance model. Within the cybersecurity field the Multistakeholder Governance Model is often utilized in formal governance settings, such as the case with IANA, ICANN, IGF, and WSIS. "No other governance model can deter the fragmentation of the Internet into jealously guarded, national telecom-run fortresses..." (Patrick, 2014). As the Internet is decentralized for the most part, control is brought on by collaborative efforts and measures. This collaboration is what makes the multistakeholder model effectiveness in answering such issues. "In areas such as security, privacy, connectivity, and human rights, it is clear that no single viewpoint can solve borderless and multidimensional issues. Instead, a more collaborative, multistakeholder approach used to tackle global Internet-related issues, such as security ones on spam and botnets, is rapidly becoming a best practice." (Internet Society, 2015, p. 2).

We can define the multistakeholder governance model as "…two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules." (Raymond and DeNardis, 2015, p. 574). Ultimately the multistakeholder model can be utilized as a tool to help facilitate dialog between actors on multiple levels, and deriving solutions to problems based on a consensus of participants or derived from evidence. Despite the value that multistakeholderism has, it's important to remember that it needs practical application to work.

Multistakeholderism relies on the interconnectivity of many partners to provide the best solutions. This primarily works on the premise that states are the main security providers. Due to the nature of the Internet being supported by non-government entities, it makes sense to include them at the table with states. Though their role may take a passive role as a spectator or become a participant in the dialog, it's important that they participate as they are consumers of the internet. (Lak, 2009, p. 5-6). Further, this inclusivity helps to create

stronger agreements overall, compared to other governance measures. With the FCC, the choice to include businesses, organizations, and citizens, shows that their decision would be weighed in accordance to all of the party's needs. "Collaboration involves joint ownership of decisions, meaning that participants are directly responsible for reaching agreement…in collaborative agreements the involved stakeholders impose decisions upon themselves." (Dewulf, 2007, p. 2). Although the FCC had the final decision, the evidence submitted for review helped to determine that outcome. Although the ISPs may have benefited from the 2018 ruling, they ultimately are agreeing with the US government that they would provide the best possible security and be open to scrutiny. The decentralized power of multistakeholderism works as it gathers a group of actors that relate to a subject, in order to obtain a balanced view and outcome. (Hoffman, 2016, p. 32). This balanced approach is what gives multistakeholderism strength as it is not one group that imposes their own beliefs; rather it's a joint effort. Additionally multistakeholderism works well on an international level, where intergovernmental diplomacy may not be a solution when there are multiple factors to a problem. (Ibid).

The traits that make up a multistakeholder governance model shows that states can share the burden of Internet governance by providing inclusivity to multiple states, while simultaneously including non-state actors to voice their opinions and concerns. Considering non-state counterparts generally have more control over the development and application of the Internet. This plays an even greater role in cybersecurity as cyber policies can affect the security of Internet users. Allowing for all information to be presented and presided over in a multistakeholder setting ensures for the best possible outcome.

We can clearly see that multistakeholderism and SAE may be compatible together as they both have similar goals. First, we must recognize that they both work best when there are multiple parties. SAE as a tool seeks the opportunity to find participants to create a narrative. Multistakeholderism offers the platform for those parties to meet on equal terms. Similarly, SAE pushes to address or discover the issues that affect individuals. Multistakeholderism would offer the best platform to develop that conversation as it's not limited to states only. Additionally, this places less burden on one party to make a decision as the conversation is developed and concluded based on disseminating and concluding all information. Although the FCC is a governing body that imparts rulings on issues, the way in which they operate is that of multistakeholderism. In that they gather experts, businesses, and testimonies help make their decision.

5. Method and Research Design

5.1 Research Design

The basic design of my thesis is of a qualitative case study, where I will be utilizing the FCCs 2018 *Declaratory Ruling, Report and Order, and Order: Restoring Internet Freedom.* It's main focus is on the removal of net neutrality principles, imposing of light-touch regulations on ISPs, and the reclassification of internet service. By analyzing the reasoning and effect of dismantling net-neutrality measures, I will be able to get a better understanding of how citizens are affected by this case. Robert Stake identifies this as an intrinsic case study, due to my interest in a specific case. "Here, it is not undertaken primarily because the case represents other cases or because it illustrates a particular trait or problem, but because, in all particularity *and* ordinaries, this case itself is of interest." (2000, p. 437). I am interested in how a specific policy is transferred from state regulated security to a market based approach, and how this might affect citizens. Focusing on a specific event, I will be able to follow the intricacies of the case more closely, compared to having multiple case studies on one subject. My research will have a generalized approach to analysis for the reader to gain a better understanding of the material in a smaller span of time. "Thus researchers use the methods for casework that they actually use to learn enough about their cases to encapsulate complex meanings into finite reports – and thus to describe the cases in sufficient narrative so that readers can vicariously experience these happenings and draw conclusions…" (Stake, 2000, p. 439). Although my goal is to find out the specifics of the *Restoring Internet Freedom*, I will also be analyzing the value of my theoretical tools and the possibility to broaden the theoretical tool in its application.

The case study will be conducted as an Issue Evolution Study, organized on a topic issue, foreshadowed problem or statement of issue, issue under development or research question, and assertion or outcome. "Issues are chosen partly in terms of what can be learned within the opportunities of study." (Stake, 2000, p. 440). As I was aware of the issue of net neutrality, I was curious to understand how the FCC came to the conclusion that light-touch regulation was a better form of security, and how they came to that conclusion despite the call for stronger net neutrality measures. Since I knew what I would be studying as my case, as well as utilizing all gathered information in my analysis, it seemed most logical to follow an issue based study. When conducting my research it's important to show accuracy of my data and interpretation for the reader. To lower the chances of miscommunication I triangulated my information. "Triangulation has been generally considered a process of using multiple perceptions to clarify meaning, verifying the repeatability of an observation or

interpretation." (Stake, 2000, p. 443). I did this by using multiple reports and articles that spoke on similar subjects, such as the effect on citizens and data pertaining to internet usage by citizens.

5.2 Analyzing the FCC

I will be looking at the United States of America and the decision to dismantle net neutrality and cybersecurity governance as the subject of study. My case study is based on the analysis of the legal document by the FCC, the declaratory ruling *Restoring Internet Freedom*. The ruling was formally adopted 14 December 2017, but released 4 January 2018, becoming a federally recognized legal document. Within *Restoring Internet Freedom*, the document outlines the goals, reasoning, and process, in removing the FCCs previous *NPRM: Preserving the Open Internet Broadband Industry Practices,* (2009), and *In the Matter of Protecting and Promoting the open Internet,* (2015). *Restoring Internet Freedom* reclassifies internet services as an information service, re-implements light-touch governance regulations, and the transfers formal oversight from the FCC to the FTC. I chose to focus on this legal document as my primary source as it presented a legal shift of cybersecurity between government regulated to market regulated internet, and the development of that policy over time. A judgement that the US government or individual states may not legally guarantee the security of citizen access or privacy while engaging the internet.

5.3 Theory Guided Case Study

The goal of this thesis is to analyze the effect of the FCC decision to remove net-neutrality, and instead focus on a market driven approach to providing cyber security in the US. Although I won't be creating or testing theories based on the research, it is still possible to utilize the critical security studies emancipatory practice as a tool to analyze the security that may, or may not, come from the FCC ruling. Florian Kohlbacher has noted that within the practice of qualitative content analysis, a case study that is backed up by theory can help analyze the material in a more comprehensive manner. "…an essential feature of theory building is comparison of the emergent concepts, theory or hypotheses with the extant literature because tying the emergent theory to existing literature enhances the internal validity, generalizability, and theoretical level of theory building from case study research." (Kohlbacher, 2006). The tool of emancipation can be applied by analyzing my data for the accuracy of the presented information in my case, compared to findings in data, historical

issues pertaining to ISP practices, and how citizens relate to the internet. Rather looking to a theory as a solution, hoping the data fits a set of parameters for a positive result..

An emancipatory practice analyzes structural constraints that impede an individual's ability to live freely through a security discourse, in which a referent object is identified with its security issue. This understanding goes onto help us understand how Laura Shepherd utilizes emancipation as an analytical tool. By analyzing who is implicated as the referent object, their claim, and where they fit within the problem. How the security issue is affecting the referent object. Lastly identifying whether the change to the security issues will provide more or less security. In the case of the FCC, the first goal is to identify the different parties and where they stand, followed by understanding how dismantling net neutrality affects them, with a final conclusion of whether if the new change is better for the referent object or not. Thus my analysis will look at whether *Restoring Internet Freedom* has created more or less security for US citizens. This will also be the point in which security as emancipation can be analyzed to understand if the theory can incorporate the securitization of the Internet, aside from traditional securitization role it currently holds.

5.4 Data Collection

The research within this thesis is based on the analysis of primary official documents provided by the Federal Communications Commission *Declaratory Ruling, Report and Order, and Order: Restoring Internet Freedom* (2018a). The data within this document is specific in how the security of the Internet will be achieved on a legal basis. Secondary sources will be utilized as well to help build a greater understanding of the decision, as well as their effects. I have 51 secondary sources from polls, statements, reports, and news sources that provide information for a better understanding of what has occurred within the ruling. Of the secondary sources they can be categorized as legal documents, human interest, data, and general fact reporting.

The legal documents provide a historical background on previous proceedings that pertain to the main case document. This includes the FCC (2014, 2015 & 2017), U. S. Const. amend. XI, § 2, Harvard Law Review (2018), Justia Law (2018), and Indiana University Law (Cannon, 2002). As these sources are based on legal documents it is less likely to be affected by partisanship.

As my study looks at how the new ruling affects citizens I felt it appropriate to look at information pertaining a human element. Sources by Holmes, et. al. (2016), Craig (2017),

Mitchell (2017), Malone (2017), and Savov (2018), are a sample of how an absence of net neutrality can affect individuals in the US and on an international level. Although a majority of human based pieces are generally pro-net neutrality liberal leaning sources, they are generally backed by legitimate facts and sources to justify their claim. I avoided articles that were a mouth piece as they wouldn't provide valuable information for my analysis.

I was also curious to find out how the repeal of net neutrality would play on security concerns, For this I included sources, for example, by Gillula & Eckersley (2017), Tews (2017), Erlin (2017), and Pegoraro (2016). These sources generally speak to the actual security implications of the *Restoring Internet Freedom*, and not based on media hype. This is why I felt it appropriate to include liberal leaning sources from Tripwire and EFF, as well as the conservative leaning AEI.

It was important that I included data that represented information about usage and connectivity of the internet, which is why I included sources from across the spectrum. For example from local and federal governments NYC Mayor's Office (2018) and Ryan & Lewis (2017), private businesses Akamai (2016) and Brogan (2017), think tanks Hitlin, et. al. (2017), and bi-partisan organizations Dean (2018). For a majority of these sources the information is based on factual findings and non-partisan. I do recognize that the private businesses and bi-partisan organizations will have an agenda, however after analyzing their data it reflected the needs of multiple points of view, or at least base their reporting on data that can be retrieved or recreated.

Finally a majority of my data can be categorized as general information pertaining to the evolution of net neutrality and general information pertaining to my case. These sources primarily are from news sources and may be liberal leaning as an organization, but the authors of each piece do a good job at capturing the general findings related to the rulings for readers to have a greater understanding. Some examples of this are by Kastrenakes (2015 & 2017), Bettilyon (2017), and Hansell (2005).

5.5 Qualitative Document Analysis

In order to complete the task of analyzing all of the captured data, I utilize Qualitative Document Analysis (QDA) as my approach for analysis. Altheide and Schneider (2013) note the general process of QDA is centered on five general steps of analysis. In QDA we start with the gathering of data from different sources. (Altheide and Schneider, 2013, p.40). Followed by creating a protocol for the analysis of documents, by asking how the source fits

into the narrative and what it provides. (Altheide and Schneider, 2013, p.44). We can then code gathered data by categorizing the information, signaling what should be incorporate the data within my analysis. Next we conduct the analysis of the codified data. They mention the goal of analysis is primarily to "…capture the meanings, emphasis, and themes of messages and to understand the organization and process of how they are presented…that we include the widest range of relevant messages in our sample." (Altheide and Schneider, 2013, p. 55). The analysis is also aided by my theoretical approach, as mentioned before in Chapter 4.3 Security as Emancipation. The finally we take the analyzed material and transfer it into report. This is conducted by summarizing each category or theme gathered from the documents, as well as questioning the importance of the data as well as how it fits within to the overall research.

5.6 Research Quality

When conducting research we must be aware of the quality of the information that we are gathering in order to produce trustworthy analysis. We can ensure the trustworthiness by holding our research to a higher level of criteria based on the validity and reliability of that data. When we carry out validity and reliability, we must keep in mind that the expectations of a qualitative study are different to that of a quantitative study. The main difference is that a qualitative study uses less physical measurements and more mental or perceptual sources of data, which take on a different meaning when evaluating the sources. "…the terms Reliability and Validity are essential criterion for quality in quantitative paradigms, in qualitative paradigms the terms Credibility, Neutrality or Confirmability, Consistency or Dependability and Applicability or Transferability are to be the essential criteria for quality." (Golafshani, 2003, p. 601).

"Although the term 'Reliability' is a concept used for testing or evaluating quantitative research, the idea is most often used in all kinds of research. If we see the idea of testing as a way of information elicitation then the most important test of any qualitative study is its quality. A good qualitative study can help us 'understand a situation that would otherwise be enigmatic or confusing'." (Golafshani, 2003, p. 601). In a quantitative study, the reliability of a set of data is determined on the accuracy and source of how that data was collected. In a qualitative study the reliability of the data gathered is determined on the basis of the dependability and consistency of the data. By ensuring the data is from sources that are reliable, it also extends credibility to the research.

This would mean then that the validity of ones data plays into the reliability of the research. “The concept of validity is described by a wide range of terms in qualitative studies. This concept is not a single, fixed or universal concept, but ‘rather a contingent construct, inescapably grounded in the processes and intentions of particular research methodologies and projects’.” (Golafshani, 2003, p. 602). Although we can’t utilize a measurement, we can determine the validity of a body research by evaluating quality or trustworthiness. If we can trust the source and information gathered, it can have a positive effect on the perception of the researchers body of analysis.

The primary document that I centered my case study on was the FCCs *Declaratory Ruling, Report and Order, and Order: Restoring Internet Freedom.* (2018a). This source is reliable as the main source is directly from the FCC, which determines that it is a valid source for analysis, while my secondary sources provide a greater analysis of the primary document. Due to the subject I have sourced literature that is not often utilized together in an academic study. The focus in cybersecurity has its own issues as sources are either focused on a theoretical perspective, or the analysis of real world situations. Due to my particular case I needed to utilized sources that are considered untraditional for my analysis. I have gathered 51 secondary sources and noted that they fall into seven originating sources: government, education, news media, op-ed, private companies, non-profit, and special interest.

Of my sources, six of them are related to the government. I obtain information from federal agencies, such as the FCC, US Census Bureau, US Department of Commerce, as well as published data from New York City’s Mayor Office. I sourced material from C-SPAN which provides public access to federal proceedings. Additionally, I consulted the US Constitution to provide an accurate understanding of states’ rights in accordance to that of federal statutes. I would consider these trustworthy sources as they provide information from firsthand source material. As a government related source they must provide truthful evidence, otherwise it undermines their authority.

Educational sources are from Indiana University Law, Harvard Law, and Justia Law. Indiana University Law provided a historical look at the historical Computer Inquiries by the federal government, which developed the telecommunications and computer network definitions used today. Harvard Law and Justia Law provide a repository for past cases, such as *FTC v. Wyndham Worldwide Corp.*, and *United States Telecom Assoc. v. FCC, No. 15-1063 (D.C. Cir. 2016).* As these sources provide access to well publicized events, we can then assume that they are reliable.

News media content is by far the largest component of secondary sources, with 22 different articles from 12 news media sources. These sources provide relevant information on FCC proceedings, legislation, analysis of events, and reported effects of both light touch regulation and net-neutrality. News media as a source can become complicated as the material can be politicized. In a 2014 study on political biases in US industries, Crowdpac found newspapers & print media, and technology industry fell more in line with liberal biases. (Shim, 2014). To understand this bias, Vanessa Otero categorized media sites based on quality and of reporting and partisan bias. Of my news sources on her chart, Reuters, The Washington Post, Time, and New York Times, generally run from minimal partisan to skewing liberal, and either providing original facts or complex analysis. (Otero, 2017). While collecting material I looked for fact based reporting as it would be less politicized and considered more reliable. Of the 12 news sources, Ars Technica, The Verge, TechCrunch, Engadget, and Inverse, provide a bulk of the articles as they largely report on issues related to the technology industry. While Free Press, Yahoo Finance, and FiveThirtyEight reports on the availability and access to internet, they utilized firsthand accounts and studies to back up their claims.

Generally op-eds are partisan based with the authors interest in swaying the opinion of the reader. Although the piece by Bettilyon (2017) was published in *Medium,* a left leaning op-ed site, he presented a historical account of how network neutrality came to be and had only reported the facts in a clear and concise manner; which is why I felt it was appropriate to use.

Material from private companies can also problematic as they may have an agenda, or may have an intention of recruiting new clients. I decided to a report from Akamai (2016) as the information regarding internet usage was based off data that they accumulated from their servers. Tripwire (Erlin, 2017) is more concerning as they are a company that serves security and IT needs of the government, reporting on the possible effects of cybersecurity if net neutrality was removed. This could be seen as a way to drum up business, but I did find news sources speaking on the subject, and felt that a direct source within the cybersecurity would be more valid and reliable to judge the situation.

When we consider sources from a non-profit we should be aware of the political leanings, as many non-profits have their own agendas and ideologies. However many of these non-profits are registered as a 501(c)(3) as it helps to reduce their operating costs. In order for this to occur, the Internal Revenue Service (IRS) requires that "…an organization must be

organized and operated exclusively for exempt purposes set forth in section 501(c)(3), and none of its earnings may inure to any private shareholder or individual. In addition, it may not be an action organization, i.e., it may not attempt to influence legislation as a substantial part of its activities and it may not participate in any campaign activity for or against political candidates." (IRS, 2018). This would mean that a non-profit could present information that supports a topic, but not actively engage to change the status quo. If the non-profit, is a reputable source we must also consider that what they present has some truths as their reputation could become damaged if not providing the best material. In my case I have included sources from nine different non-profits, covering 13 articles and reports. The Pew Research Center is non-partisan and does in-depth analysis of subjects with the aim to find truth; Pew had a focus on the individuals and how they interacted with the internet. Although the National Conference of State Legislatures is a non-governmental organization, they do conduct bi-partisan research. However in my case I utilized information pertaining to state support for net-neutrality. (Dean, 2018). However organizations like the Electronic Frontier Foundation, Center for Public Integrity, Institute for Local Self Reliance, and the American Enterprise Institute do have an agenda, and conduct research to help support their stance. Despite this, I found that the information that they present is generally based on firsthand accounts or based on factual reporting. Additionally the ACLU questioned the trust of the FTC to protect consumers. What gives this source validity is that the author stakes his reputation on the number of years working within privacy issues as a consultant. (Gellman, 2016).

Finally the area of special interest can be contentious as they provide a perspective of how issues affect their organization. In *Restoring Internet Freedom*, the FCC included a report by USTelecom on how *Title II* affected ISPs and how they are able to invest. The source provided an insight into the average spending of ISPs over 20 years. As the source was based on factual numbers from the industry, we can view it too has validity.

What we must keep in mind about the use of non-traditional sources in research is that not all sources are equal. When choosing a source we must be aware of the political biases, type of source, and how they present the source.

6. Case Study: Analysis of the FCC *Restoring Internet Freedom* of 2018

6.1 Introduction

The main premise of the Federal Communications Commission (FCC) *Declaratory Ruling, Report and Order, and Order: Restoring Internet Freedom* (2018a) is one that frames

cybersecurity around the idea citizens would be better cared for under a market driven solution, in which minimal government oversight and regulations are applied to internet service providers. Prior to the new regulatory ruling, in 2015 the FCC passed regulations under the *In the Matter of Protecting and Promoting the open Internet.* This became known as the *Title II Order*, which classified broadband providers as a telecommunications service since they did not meet the requirements of a Title I information service. This was also an extension of the *NPRM: Preserving the Open Internet Broadband Industry Practices* (2009), which originally established net neutrality rules in the US. Under the new guidance of *Restoring Internet Freedom,* the FCC re-established ISPs as an information service, brought back a light touch regulation model prior to 2009, and transferred oversight from the FCC to the Federal Trade Commission (FTC). By utilizing security as emancipation as our tool for analysis, we will be examine how the *Restoring Internet Freedom* talks about creating security for citizens. Critically analyzing the points of view from the 2017 ruling will help us to understand if the FCC is indeed creating more security for citizens or for the ISPs.

The Federal Communications Commission is made of five commissioners, acting as an independent advisory board that "…regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories." (FCC, 2018b). Each member is confirmed by the U.S. Senate for a five year term; the board must have no more than three individuals within the same political party, and the chairman is appointed by the President of the United States. (Ibid). The current board consists of Chairman Ajit Pai (Republican), Commissioner Michael O'Reilly (Republican), Commissioner Brendan Carr (Republican), and Commissioner Jessica Rosenworcel (Democrat). The fifth seat is currently vacant as Mignon Clyburn (Democrat) stepped down shortly after the approval of *Restoring Internet Freedom.* The FCC operates as a hearing committee that votes on presented information. The FCC received information and testimony during the hearing from many different sources, such as businesses, large and small ISPs, non-profits such as the Electronic Frontier Foundation and American Enterprise Institute, and testimony from United States citizens.

6.2 Rules for Restoring Internet Freedom

The FCCs *Restoring Internet Freedom* starts by outlining that their goal with this document is to reverse the *Title II Order*. "Today, we honor that bipartisan commitment to a free and open Internet by rejecting government control of the Internet. We reverse the Commission's abrupt shift two years ago to heavy-handed utility style regulation of

broadband Internet access service and return to the light-touch framework under which a free and open Internet underwent rapid and unprecedented growth for almost two decades. We eliminate burdensome regulation that stifles innovation and deters investment, and empower Americans to choose the broadband Internet access service that best fits their needs." (FCC, 2018a, p. 2). This statement helps to set the overall tone of the document, where the previous ruling from 2015 hindered the ability for ISPs to provide Internet services citizen need. The FCC motions that the new declaratory ruling would change the existing definition of ISPs as a utility like telecommunication service, to that of an information services with little oversight. Both serve different purposes and follow different guidelines. The FCC sees this new ruling working towards a better system. "Over twenty years ago, in the Telecommunications Act of 1996, President Clinton and a Republican Congress established the policy of the United States 'to preserve the vibrant and competitive free market that presently exists for the Internet . . . unfettered by Federal or State regulation'." (FCC, 2018a, p. 2). Within the first page of their introduction they are driving their opinion across that under *Restoring Internet Freedom* ISPs are now considered an information service, which subjects them to less regulation, freeing them to conduct business, benefiting citizens. Further, the FCC sees their actions as a bipartisan effort like that of the *Telecommunications Act of 1996.*

The FCC concludes by outlining the three steps under their new light-touch regulation. This explains how the FCC and ISPs will work together, the transition of ISPs to an information services classification, and how this will be beneficial to consumers. "Through these actions, we advance our critical work to promote broadband deployment in rural America and infrastructure investment throughout the nation, brighten the future of innovation both within networks and at their edge, and move closer to the goal of eliminating the digital divide." (FCC, 2018a, p. 3)

The FCCs first goal is to implement market based policies, and to end utility style regulation. They claim a light-touch information service framework will "…promote investment and innovation better than applying costly and restrictive laws of a bygone era to broadband Internet access service. Our balanced approach also restores the authority of the nation's most experienced cop on the privacy beat—the Federal Trade Commission—to police the privacy practices of (ISPs)." (FCC, 2018a, p. 2). It's believed that *Title II* made it difficult for companies to innovate and provide service for people as ISPs had limitations on how they could operate. To regulate ISP, the FCC believes that the FTC would be more appropriate. David Shepardson reported that FCC Chairman Ajit Pai stated the two agencies

would "…work together to take targeted action against bad actors." (2017). Instead, under the new light touch framework, Ajit Pai expects the FCC to "…no longer bar any specific Internet provider practice but require companies to disclose if they block, throttle or offer paid prioritization of Internet traffic." (Ibid). Additionally FCC Commissioner Jessica Rosenworcel sees that the FTC would be inadequate at providing the correct protections as "FTC enforcement would happen long after the fact — many months, if not years, after consumers and businesses have been harmed." (Ibid). In reality what this does is it allows ISPs to self-regulate which is what led the FCC to create the *Title II Order*. According to Robert Gellman, a privacy and information consultant of 40 years, he feels that the FTC is inadequate in proving proper online protection. "Unlike the FTC, the FCC has lots of regulatory authority with respect to telecommunications carriers, and its current effort to write privacy rules for companies that provide broadband services is a much-needed exercise of that authority…business interests see the FTC as a weaker regulator than the FCC." (Gellman, 2016).

However, in the 3rd U.S. Circuit Court of Appeals of Philadelphia, they have previously ruled in favor of the FTC on grounds that they have regulatory authority of cyber security cases. (Stempel, 2015). In 2008 and 2009, the Wyndham Worldwide Corp. lacked cyber security measures resulting in a data breach. (Ibid). But in this case the FTC only filed suit until June 2012, resolving the case in 2015; taking seven years to resolve this case. (Harvard Law Review, 2016). On the other hand a regulatory shift in authority to the FTC would allow for greater legal precedence in the face of a lawsuit. Regardless the *FTC v. Wyndham Worldwide Corp.* case proves FCC Commissioner Rosenworcel correct in terms of timing of enforcement. Moreover, the light touch regulatory framework that was adopted would further hinder the FTCs enforcement capabilities.

Their second objective determines light-touch regulations, asking for ISPs to be transparent in the operation. "Disclosure of network management practices, performance, and commercial terms of service is important for Internet freedom because it helps consumers choose what works best for them and enables entrepreneurs and other small businesses to get technical information needed to innovate." (FCC, 2018a, p. 3) This indicates that the decision to work with an ISP is dependent upon a citizen's ability to compare services, and that dictating how an ISP operates will only diffuse competition. This would mean that ISPs would have to operate openly to allow customers to be well informed, which means ISPs are expected to self-report on all activities. The problem with this is that even under net neutrality rules ISPs were found to be hindering services to their customers, knowingly and

unknowingly. In a report from the Institute for Local Self-Reliance on the two biggest cable and telephone companies in the United States, they found "AT&T exempted DirecTV from its data caps; AT&T and Verizon on data cap exemptions; Verizon throttling Netflix; Verizon Lawyer tells federal court it wants paid prioritization; Comcast removes pledge against paid prioritization; Charter messes with inter-connection points to create fast lanes. There is more - such as Comcast's throttling BitTorrent while lying to subscribers about it." (Mitchell, 2017). This becomes further problematized when broadband coverage in areas is limited to a few providers, where more than 19 million people are limited to a single provider for broadband, with a minimum speed of 25 Mbps download and 3 Mbps upload, and that about 52 million people have internet services from a company that has violated network neutrality laws in the past. Even among 146 million customers who can choose between at least two providers, a third of them will sign on with an ISP that has violated network neutrality. (Ibid). What this means is that even under ideal conditions, most households will be able to only choose between one or two companies that have been known to previously flaunt the law; which questions the trust of ISPs under the new light-touch regulations.

In a 2014 study of broadband speeds by the U.S. Department of Commerce (DoC) Economic and Statistics Administration, they found that broadband competition decreases as broadband speeds increases, which they found that "having fewer competitors at a given speed is likely to drive up prices. As a result, some consumers will decide not to adopt Internet access at all, some will choose a slower speed that otherwise, and some will economize in other ways." (Beede, 2014, "Executive Summary" para. 6). The 2014 report also found that about 29% of households at the time did not have Internet service due to high costs, and that when ISPs have less competition they are more likely to increase prices, which reduces "…product quality or variety, service, or innovation." (Beede, 2014, p. 1). The answer to providing better service and more innovation is incentivizing competition for ISPs. When Google Fiber started providing 1000Mbps service within the Kansas City, Missouri, AT&T announced they would be offering an equivalent service with competitive prices; an upgrade to their existing service prior to the presence of Google. "… when it comes to giving consumers what they really care about—how well their favorite sites perform—the only sure fix is to make companies fight over your business. In Kansas City, AT&T may have been able to provide better service, but it saw no reason to make the effort until another company's offering threatened to siphon away paying customers." (Davidson, 2015).

The last rule in *Restoring Internet Freedom* eliminates the conduct rules established under *Title II*. They believe that regulations set under a telecommunication services are

unnecessary due to their transparency requirements and the available suite of antitrust and consumer protection laws, which would provide adequate protection in the event that ISPs go against open internet principles. (FCC, 2018a, p.3). The FCCs *Open Internet Order* conduct rules for ISPs declared no throttling, blocking, or paid prioritization, this also included "…no unbundling of last-mile facilities, no tariffing, no rate regulation, and no cost accounting rules, which results in a carefully tailored application of only those Title II provisions found to directly further the public interest in an open Internet and more, better, and open broadband…" (Kastrenakes, 2015). The FCC justifies the abandonment of the 2015 rules as the benefits come at the cost of innovation and investment by ISPs, and the belief that the FCC held no legal authority over ISPs to enforce net neutrality rules. (FCC, 2018a, p. 3). However Ars Technia reported that former FCC Chairman Tom Wheeler spoke at a forum criticizing this move, stating that reclassifying ISPs under *Title II* as telecommunications companies was "…the best legal authority the FCC could use to protect net neutrality and consumers." (Brodkin, 2017b). Wheeler explained further for their reasoning for invoking *Title II*, saying they would be able to impose net neutrality rules against blocking, throttling, and paid prioritization, and to "…impose tough online privacy rules on ISPs and to let the FCC impose a 'general conduct standard' to stop anti-consumer behavior that isn't covered by the core rules…" (Ibid). It's not the fact that the FCC has overall legal authority to hand down fines, it's that *Title II* provides a parameter in which ISPs are able to operate within, and how infractions by ISPs would be handled.

Additionally, the EFF reported that 40 plus small ISPs wrote to FCC Chairman Pai, expressing approval of the 2015 *Open Internet Order*, noting net neutrality "…hasn't hurt their ability to develop and expand their networks." (Falcon, 2017). In the letter they express net neutrality rules address the anticompetitive practices of ISPs, whereas *Restoring Internet Freedom* threatens competitive entry viability. As they are smaller cable and telephone companies, net neutrality rules help to restrain the ability of ISPs to monopolize the market. (Ibid). Effectively *Restoring Internet Freedom* would allow large ISPs to block edge providers utilizing infrastructure if they are in direct competition. Although it's anticompetitive, the FCC views this as the market working for customers. When the FCC enacted *Title II*, it allowed thm to "…intervene to prevent a major ISP with a vast network from leveraging its massive network size in an anti-competitive way to harm other networks." (Ibid). Now that the FCC has moved forward to dismantling the *Open Internet Order*, the original protections that allowed the FCC to manage and challenge ISPs, now falls to existing antitrust and consumer protection laws provided by the Bureau of Consumer Protection,

which operates under the FTC. As mentioned before, the FTC would be ill equipped at providing protection for consumers; effectively removing any regulatory measures to keep ISPs in check.

6.3 Historical Rulings as Background

The *Restoring Internet Freedom* explains how they came to the interpretation that ISPs should be considered information service. However we should understand why the FCC classified ISPs as a telecommunication service in the first place, by historically analyzing how the FCC classified communications

Regulations of communication by the United States government was first introduced by the *Communications Act of 1934*, establishing the FCC. *Title II* regulations were created and upheld by Common Carrier laws, which are essential for net neutrality measures. Common Carrier, or Common Carriage, was first applied in 1887 to railroad services, whereby rail carriers could not discriminate against individuals or types of cargo, and that all services must charge a standard rate. Prior to the *Communications Act of 1934*, the Bell System telephone company (later AT&T) was the largest telephone company with the ability to manipulate the market by economic means, forcing smaller telephone companies to fold and sell their infrastructure primarily to Bell System; essentially monopolizing the market. With the Bell System controlling most of the market, the cost of maintenance and expansion into rural areas was too much of an investment and was left undeveloped, leaving rural areas without service. The introduction of *Title II* forced telephone companies to provide service in areas that weren't previously covered, benefitting citizens and improving the telephone system. The overarching goal of the Act was to provide a universal service to all citizens; equality. This was achieved in two ways. "First, AT&T would have to submit to regulation of the rates they can charge customers; the government was to ensure that all Americans were paying the same, fair, price. Second, AT&T would have to interconnect with smaller services in rural areas…The act required AT&T to provide would-be-competitors access to their infrastructure in the interest of universal service." (Bettilyon, 2017). There are clear similarities of the Bell System and current ISPs. In rural parts of the United States, ISPs may not provide similar services or infrastructure to that of more populated areas as the cost to providing service to a smaller population yields less profit. If left out of serviceable areas, not only does this mean that individuals in rural areas tend to get poorer service, we see that this inadvertently affects how people conduct business, access information, and the education of individuals in these areas. According to the FCC, large portions of the United States are left

without service. "…39 percent of rural Americans — 23 million people — don't have access. In Pew surveys, those who live in rural areas were about twice as likely not to use the Internet as urban or suburban Americans." (Malone, 2017). The Center for Public Integrity also found that low income households are at a disadvantage in acquiring broadband. "…rural poor are still in excess of one-and-a-half times as likely to lack high-speed broadband as rural wealthy families. Even in urban areas where 94 percent of households have access, low-income families are three times as likely to lack access as the wealthiest urban families…" (Holmes et al., 2016). Within cities there can be inequality of service as ISPs may agree to divide a city into service areas. Operating in specific areas might allow an ISP to focus and deliver better products, but it can also force citizens to have fewer choices or none at all. A 2018 report by the City of New York found that "…More than two thirds of households (69%) and nearly three quarters of small businesses (72%) have only one or two options of broadband providers." (NYC Mayor's Office of the Chief Technology Officer, 2018). If the *Open Internet Order* were to have fully flourished, these areas would have seen an increase in competition, as well as the expansion of networks to meet the needs of areas that are underserved. By defining ISPs as information services within *Restoring Internet Freedom*, existing ISPs are not held to the standard of common carrier laws. The reason the FCC reclassified a broadband service as an information service is the perception that ISPs only provide the ability to connect to the internet and transmit data from user to end user. While the transmission of data is similar to that of a telephone service, the main difference is that requested data does not have a set path when reaching an end user, unlike a telephone address that has a direct address.

To understand the 2018 decision, we must understand Internet usage as defined by the *Telecommunications Act of 1996*; which defines the difference between a telecommunication service and information service. *Restoring Internet Freedom* also updates the definition of an "interactive computer service" to include "…any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet . . . ." (FCC, 2018a, p. 4). Here we can see this is contextualizing that telecommunications and information services are connected, but we must keep in mind that this definition of an ISP is over 20 years old. At the time ISPs only produced access to broadband internet, compared to today where they might produce content or provide a platform for content; such as Comcast owning NBCUniversal or Verizon and its Go90 video streaming app. The FCC looks back at

to the *Telecommunications Act of 1996* as a moment that allowed the Internet to flourish. "For the next 16 years, the Commission repeatedly adopted a light-touch approach to the Internet that favored discrete and targeted actions over pre-emptive, sweeping regulation of Internet service providers." (FCC, 2018a, p. 4). However according to Rob Pegoraro, technology reporter 1999-2011, the FCC might be viewing history from rose tinted glasses. "Without government oversight, phone companies could have prevented dial-up Internet service providers from even connecting to customers. In the 1990s, in fact, FCC regulations more intrusive than the Obama administration's net neutrality rules led to far more competition among early broadband providers than we have today." (Pegoraro, 2017). Even if light touch regulation were better than the 2015 utility style regulations, former FCC Commissioner Mignon Clyburn wrote in her 2018 dissent of *Restring Internet Freedom,* stating that she saw no evidence to support the claim that the 2015 ruling had hindered ISPs. "…we have seen self-serving statements from broadband providers that our net neutrality rules have somehow hamstrung them from bringing 'innovative' new offerings to market before. But they never did tell us what those offerings would have been at any real level of detail. My view is that if there indeed were innovative offerings that would have garnered any real consumer interest, the better course would have been to make those ideas public, and let consumers badger the contrarian FCC into submission." (FCC, 2018a, p. 225). The claim by broadband providers that Title II harmed their ability to invest in innovate was also found to be false by Free Press, a media reform advocacy group. "We found that not a single publicly traded U.S. ISP ever told its investors (or the SEC) that Title II negatively impacted its own investments specifically." (Turner, 2017, p. 10). Their findings showed that investments and expansion increased following the *Open Internet Order,* "During the two years following the Open Internet Order vote, cable-industry physical-network investments increased 48 percent compared to the amount invested during the two prior years. Cable's core network investments accelerated dramatically during 2016 (a $2.1 billion increase over 2015, compared to 2015's $0.8 billion increase over 2014)." (Turner, 2017, p. 6). If broadband providers were able to continue investing and expanding their networks, we have to wonder why there is a problem and who really benefits from the removal of Title II regulations.

In 1998 the *Stevens Report* was critical in determining the definition of an information service, and was used as evidence for support of the 2018 decision. The report "…comprehensively reviewed the (Telecommunications) Act's definitions as they applied to the emerging technology of the Internet and concluded that Internet access service was

properly classified as an information service." (FCC, 2018a, P. 4). This helps to explain their motivation and interpretation for changing the designation of the Internet from a telecommunications company under *Title II*, back to an information services. Reclassifying under the new ruling would create less constraints on the Internet Service Providers, however it would also repeal protections for consumers that were designated after previous infringements by ISPs. Instead it was expressed in the Stevens Report that "…'the broad range of Title II constraints' would 'seriously curtail the regulatory freedom that the Commission concluded in *Computer II* was important to the healthy and competitive development of the enhanced-services industry." (FCC, 2018a, p. 4). What they are referring to in the Computer II inquiry of 1976, was the FCCs move to define a communication service versus a data services. A communications service was considered a basic level entity that encompasses communications by phone, as well as products that worked with those services. The second category of Enhanced Service Providers, or data services, were considered "…[S]ervices, offered over common carrier transmission facilities used in interstate communications, which employ computer processing applications that act on the format, content, code, protocol or similar aspects of the subscriber's transmitted information; provide the subscriber additional, different, or restructured information; or involve subscriber interaction with stored information." (Cannon, 2002, p. 185-186). Cannon explains that the classification of enhanced services placed an emphasis on the actions involved with data processing to help differentiate that from basic services. "The basic versus enhanced dichotomy was designed as a bright-line test, eliminating the 'hybrid' middle ground and case-by-case review. Enhanced services are anything more than the transmission capacity of basic service." (Cannon, 2002, p. 186-187). Although they are correct in identifying how the FCC originally came to ruling of basic and enhanced services, the issue becomes complicated when ISPs merge or vertically integrate their products, and when data routed through telephone cables. When ISPs vertically integrate their products, such as video calling and instant messaging, it's hard to draw a line between communication and information services.

Historically, the FCC has reclassified Internet services as an information service in the past, as what happened in 2002 with the ordering of broadband services as an information service]. Under the 2002 *Cable Modem Order* "…the Commission classified broadband Internet access service over cable systems as an 'interstate information service,' a classification that the Supreme Court upheld in June 2005 in the *Brand X* decision. There was no dispute that at least some of the elements of Internet access met the definition of

‘information services,’ and the Court rejected claims that ‘[w]hen a consumer goes beyond those offerings and accesses content provided by parties other than the cable company’ that ‘consumer uses ‘pure transmission’.” (FCC, 2018a, p. 5). What this demonstrates is that, again, in previous court rulings it was found that ISPs were classified as information services as they provided access to the Internet and the service of routing customers to third parties. Whether that is a website or an email service, the ISP doesn’t own the end product, instead providing the means to access the internet and connect to third parties. But what the FCC isn’t considering is how the internet and ISPs have changed, and where the line is drawn between information services and content producer lies. For example, Verizon Communications created and maintained the go90 video streaming platform from 2015 to 2018. They bought and leased content, as well as production companies, to fill their platform. During its tenure, it was found that Verizon was deliberately throttling user experience with Netflix and YouTube (Brodkin, 2017a), and not capping customers data if utilizing go90 services (Sottek, 2016). In 2011, Comcast’s acquisition of NBCUniversal gave them a foothold in the U.S. media market. The merger came with a stipulation by the FCC and Department of Justice in which Comcast was not allowed to discriminate against competitors or prioritize their content over others; built on the trust that they would abide by. (Brodkin, 2018). The concern here is whether we can trust ISPs to treat all data fairly in accordance with *Restoring Internet Freedom*, especially when they are financially incentivized by their own media ambitions.

Although much of the conversation by the FCC focused on the classification of ISPs, they did recognize that customers have inherent rights when accessing the internet. In 2004 the FCC created the four principles for internet freedom, creating open innovation with minimal regulations. “These four ‘Internet freedoms’ include the freedom to access lawful content, the freedom to use applications, the freedom to attach personal devices to the network, and the freedom to obtain service plan information.” (FCC, 2018a, p. 5). This alludes to the how they perceive the Internet should function as a main priority. In 2007, a challenge was made against the 2002 classification, but FCC found ISPs to be an information service, which resulted in the *Wireless Broadband Internet Access Order.* They use this as an example to help show that there is a historical importance to their 2017 decision. “…the Commission classified wireless broadband Internet access service as an information service, again recognizing the “minimal regulatory environment” that promoted the “ubiquitous availability of broadband to all Americans.” (FCC, 2018a, p. 6). This was the first time they spoke about how this past FCC decision benefited the American citizen in *Restoring Internet*

Freedom, in regards to reclassifying Internet activity from telecommunications to information services. By 2008 the FCC filed the *Comcast-BitTorrent Order,* when they found that Comcast was actively throttling peer-to-peer applications like BitTorrent, or Gnutella. The FCC enforced their order by using the *Internet Policy Statement* as a legal backing to stop Comcast from hindering customers. At the time they found that Comcast was blocking access content and applications, but this was rejected by the U.S. Court of Appeals for the D.C. Circuit in 2010, as the court saw FCC had no legal authority. (FCC, 2018a, P. 6). The FCC noted that even with the rules that they had in place, they were considered to not have the direct authority to challenge ISPs. This ruling deemed the justification as to why the FCC could not properly protect consumers, and instead would pass the responsibility to the FTC. Previous FCC Chairman Kevin Martin, 2005-2009, disagreed with this as consumers needed protection that wasn't available unless through the FCC. "While Comcast has said it would stop the arbitrary blocking, consumers deserve to know that the commitment is backed up by legal enforcement." (McCullagh, 2008). Under a common carrier law, Comcast would be obliged to transfer the data no matter the content or data size. Although the FCC tried to upheld existing rules they were impeded by congress to allow the FCC to have more strength. "In 2006, Congress rejected five different bills that would have handed the FCC the power to police Net neutrality violations; the FCC has acknowledged that its own Net neutrality principles 'are not enforceable'; the Supreme Court has previously ruled that the FCC has no power to regulate 'unless and until Congress confers power upon it'." (Ibid). What this means is the FCC is only allowed to create regulatory rulings, and if the rulings are infringed upon it would have to be congressional or judicial affair to resolve the issue. Further when we delve deeper into rulings against the FCC, under United States Supreme Court case *Louisiana Public Service Comm'n v. FCC, (1986)* we find that the FCC was deemed to have no authority at all. The court ruled that federal policies encouraging competition would be negatively impacted if the FCC had enforcement power. Instead state commissioners, as given power by Congress, would have more legal authority. They asserted this by noting that the 1934 Act doesn't grant power over states by the FCC the power. (476 US 355) Through this section we can see that the FCC has had a historical legal backing as to why the FCC should transfer the protection of consumers to the FTC.

In 2010, the FCC adopted the *Open Internet Order,* which according to the FCC utilized new regulatory authority under Section 706 of the Telecommunications Act. Establishing that ISPs couldn't blocking and or have unreasonable- discrimination rules (FCC, 2018a, p. 6). Part of this ruling, like *Restoring Internet Freedom,* pushed ISPs to

"…publicly disclose accurate information regarding the network management practices, performance, and commercial terms of its broadband Internet access services." (Ibid). In 2014, the DC Circuit, under Section 706 of the Telecommunications Act, upheld this ruling on the grounds that mobile broadband internet service was not a commercial mobile service. (Ibid). In 2014, the FCC gained more support when President Barack Obama ordered for the reclassification of broadband to that of a telecommunications service under *Title II*. Due to the new regulatory standing of the FCC, they created three bright-line rules "…prohibiting blocking, throttling, and paid-prioritization, as well as a general Internet conduct standard and 'enhancements' to the transparency rule." (FCC, 2018a, p.7). Not only did this give more power the FCC, it was also a total divergence as to how the FCC operated as a whole, paving the way for real change in net neutrality in the United States. In 2016, the D.C. Circuit ruled in favor of the FCC in *United States Telecom Association v. FCC*, where broadband internet was ruled as a telecommunications service, offering that service for a fee. "In accordance with Brand X, the Commission's conclusions about consumer perception find extensive support in the record and together justify the Commission's decision to reclassify broadband as a telecommunications service." (Justia Law, 2018). This meant the FCC had the power to regulate based on *Title II*, helping to reject two of the USTelecom's challenges. The D.C. Circuit based their support for the FCC, due to the clearly defined rules in *Title II*; no "…banning (i) blocking, (ii) throttling, and (iii) paid prioritization; (iv) a General Conduct Rule; and (v) an enhanced transparency rule." (Jutsia Law, 2018). Prior to *Title II* the FCC wouldn't have been able to step into regulate the industry and protect consumers. After implementing Title II, it was found that ISPs directly violated the five rules. Since the ISPs were notified of the new regulations prior to infringement, D.C. Circuit saw a clear breach by ISPs and that FCC was in the right of way to pursue them. Second it also showed that there can't be two different classifications for Internet providers. Comparatively in the 2005 case, *National Cable & Telecommunications Association v. Brand X Internet Services*, it labeled dial-up internet providers as telecommunications due to customers connecting directly into telephone connections. Whereas DSL providers were considered information services even though DSL utilized the same telephone hardwiring as dial-up, but utilized a modem at the customers location to split the signal as it entered the house. (Hansell, 2005). Because the court found *Title II* held merit at the time, it provided the proof for that legally the FCC has the right to protect consumers, as well as redefine what it means to be telecommunications information service.

As President Donald Trump assumed leadership, the FCC moved away from a pro-net neutrality organization, they established the *FCC Initiative – Restoring Internet Freedom* in May 2017. This proposal became the predecessor of the *Restoring Internet Freedom* "…we proposed to return to the successful light-touch bipartisan framework that promoted a free and open Internet and, for almost twenty years, saw it flourish. Specifically, the *Internet Freedom NPRM* proposed to reinstate the information service classification of broadband Internet access service. The *Internet Freedom NPRM* also proposed to reinstate the determination that mobile broadband Internet access service is not a commercial mobile service." (FCC, 2017, p. 7). Additionally within the 2017 NPRM, the FCC planned to revisit existing rules and enforcement regimes in order to understand if past regulations could be of use, such as intervention in market and ISP practices. The FCC also opened the debate by allowing public opinion as part of their inquiry into reclassification of broadband providers. "…August 30, 2017, more than 22 million comments were filed in our Electronic Comment Filing System (ECFS), with even more submissions lodged during the *ex parte* period." (FCC, 2018a, p. 8). In fact, there were so many comments regarding the subject of reclassification that the FCC was urged to make a two week extension, compared to the 2014 public comments on Title II that received only 3.7 million replies it shows that the public opinion is quite strong on the subject. (Kastrenakes, 2017). At the time the FCC thought they had suffered from a distributed denial-of-service (DDoS) attack due to the number of comments happening at one time, which coincided with John Oliver segment on *Last Week Tonight* that encouraged his audience to leave a comment with the FCC; this also occurred again in 2014 after a similar John Oliver segment. (Lecher, 2017). Although it seems like the number of comments was significant, according to the Pew Research Center approximately 57% of registered comments were from temporary emails, bulk emails, or even campaign bots. "The Center's analysis finds support for this argument, based on the fact that many comments were submitted at precisely the same instant. The FCC assigned a precise timestamp to each comment as it was submitted, and an analysis of those timestamps shows that on numerous occasions, thousands of posts were submitted at exactly the same time – a sign that these submissions were likely automated." (Hitlin, Olmstead, Toor, 2017). Former FCC Commissioner Clyburn disagreed in the FCCs ultimate choice to not include public comments on account that it may be part of an alleged attack. "I hold in my hand letters that plead with the FCC to keep our net neutrality rules in place but what is striking and in keeping with the new norm, despite the millions of comments, letters, and calls received, this Order cites, **not even one consumer comment**. That speaks volumes about the direction the

FCC is heading. That speaks volumes about just who is being heard at the FCC." (FCC, 2018a, p. 223). In the end the FCC concluded that the supposed DDoS attack was not a coordinated cyber-attack. According to the FCC Inspector General, "In fact, it was likely just design flaws in the system, paired with the increase in traffic from the John Oliver program (up 3,116 percent) that caused the system to shut down." (Kelly, 2018a). Chairman Ajit Pai was questioned prior to this revelation by Senators Ron Wyden (D-Ore.) and Brian Schatz (D-Hawaii), in May 2017. "Pai's letter to Wyden and Schatz included an attachment in which then-FCC CIO David Bray responded directly to the senators' questions. This part of the letter contained multiple false and misleading statements, according to the FCC Inspector General's report…" (Brodkin, 2018). However Chairman Pai reasoned that the FCC couldn't tell the public the truth because it could jeopardize the Investigator Generals' investigation into the supposed DDoS attack, without risking legal ramifications. (Lucchesi, 2018). If the FCC knew the attack might have been false, then we must ask why they didn't wait for the investigation to complete. If the public opinion matters as much they would have at least noted their opinions.

6.4 FCC Reasoning for Information Services Classification

Overall, the decision to change the classification of the ISPs as telecommunication services to that of information services, then relies upon the *Brand* X ruling by the United States Supreme Court. This supports the claim that a broadband, fixed or mobile, internet service is an information service, and that a mobile broadband internet service should not be classified as a commercial mobile service or equivalent. (FCC, 2018a, p. 8). Their decision to change the classification is legally allowable under their authority, which can be backed up with the numerous occasions wherein they changed classification previously. They believe their decision can be supported by public policy, as well as evidence, when an information services was perceived to be better.

> "…we find that economic theory, empirical data, and even anecdotal evidence also counsel against imposing public-utility style regulation on ISPs. The broader Internet ecosystem thrived under the light-touch regulatory treatment of Title I, with massive investment and innovation by both ISPs and edge providers, leading to previously unimagined technological developments and services. We conclude that a return to Title I classification will facilitate critical broadband investment and innovation by removing regulatory uncertainty and lowering compliance costs." (FCC, 2018a, p. 8).

Although the FCC views the return of a light touch model as a way to improve the internet, it seems they weren't considering why they originally pushed for measures that emphasized consumer protection. Instead *Title II* was seen as a way for government to involve themselves when businesses and the market could be a better provider of security. Under Section III, paragraph 21, the document defines broadband Internet access service as a "…mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service." (FCC, 2018a, p. 8-9). They continue on to define that there are two type of Internet service, fixed point of connection and mobile data, as end users will access the Internet from those two main platforms. The documents supports the idea of reclassification due to the fact that ISPs are the means for data to be transferred, and as mentioned before has been supported under past FCC regulations and judicial rulings. "Not only do ISPs offer end users the capability to interact with information online in each and every…they also do so through a variety of functionally integrated information processing components that are part and parcel of the broadband Internet access service offering itself…ISPs are integrated information processing capabilities offered as part of broadband Internet access service to consumers today." (FCC, 2018a, p. 14).

The FCC is adamant about the benefits of reclassification after speaking with customers of ISPs. They found that "…broadband Internet access service primarily is used to access content, applications, and services from third parties unaffiliated with the ISP in support of the view that customers perceive it as a separate offering of telecommunications." (FCC, 2018a, p. 13). *Restoring Internet Freedom* concludes that the primary function of the Internet is to transfer data from a user to a third party entity, such as a website or network host through the Domain Name System (DNS). "DNS is used to facilitate the information retrieval capabilities that are inherent in Internet access. DNS allows 'click through' access from one web page to another, and its computer processing functions analyze user queries to determine which website (and server) would respond best to the user's request." (FCC, 2018a, p. 16) Under the *Brand X* ruling, it's crucial to understand that DNS, is an information service as DNS is what allows for data to properly be routed by the ISP on behalf of the customer an third party. (FCC, 2018a, p. 18). We must remember that telecommunication services connect users directly to another party, as the user will personally enter a distinct a telephone number. Whereas in an information service, the user does not connect directly to an end source. Instead the website is routed through a DNS service that translates and routes

addresses automatically in the form of an IP address, directly to the correct address. This becomes more apparent as requested data may be stored in one location, but can change over time due to networks and databases propensity to be moved or upgraded. The FCC understands that the *Telecommunications Act of 1996* as a federal policy in which to "…preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." (FCC, 2018a, p. 21). This then creates precedent for the FCC to not regulate ISPs, and the reason for a return of light-touch regulation. Their use of the *Brand X* ruling further recognizes that ISPs were considered an information service all along, whereas a telecommunications service "…can reasonably be read to mean a 'stand-alone' offering of telecommunications…" (FCC, 2018a, p. 33). Despite utilizing a similar infrastructure to transmit data, the ruling showed that the ISPs were strictly dealing with information, even if they separated out the bundled service packages. "Thus, an offering like broadband Internet access service that 'always and necessarily' includes integrated transmission and information service capabilities would be an information service." (FCC, 2018a, p. 35). Essentially if we look at the service they provide, they are merely transmitting data, even if that data is carrying communicable information such as email, audio, or video communications.

At this point *Restoring Internet Freedom* appears to be less concerned of net-neutrality matters, and more about business practices and government intervention. Yet we must understand that even if reclassification fixes how we perceive the Internet, it means that we still need rules for how our data is transferred, treated, protected, and stored. What reclassifying really does is removes the capability of the FCC to regulate, which is inherent under telecommunications guidelines. This then is the crux of the problem, if you don't have any guidance or regulation, then how are you to provide the ability to protect consumers.

6.5 Claims for and against the FCC Decision

The FCC cited in their 2018 decision the findings by USTelecom. Prior to *Title II,* USTelecom found the broadband industry was funneling more money into the system to innovate and expand. During that time ISPs were encouraged to conduct broadband investment and innovation. "For almost 20 years, there was a bipartisan consensus that broadband should remain under *Title I*, and ISPs cumulatively invested $1.5 trillion in broadband networks between 1996 and 2015." (FCC, 2018a, p. 52). However when you evaluate the report created by USTelecom (Brogan, 2017), the numbers that the FCC cites are not quite showing the full picture. During the years of 2014-2016, under *Title II*, we do see

the expenditure drop from 78.4$ billion to 76$ billion, though it still outmatched spending to previous years. Comparatively between 1996 and 2014 the industry was spending an average of 73.4$ billion a year. Additionally the 1.5$ trillion of capital investments claimed to be invested over 20 years only averages to about 7.5$ billion per year. Also the 1.5$ trillion can't be differentiated from the historical capital expenditure as it's not separated out from the data, so we must assume that it's included into the reported yearly expenditures. (Brogan, 2017). In reality *Title II* has had less of an effect on expenditures by the industry than what's being presented by the FCC and USTelecom.

The FCC also provided evidence that fewer regulations had a positive effect on ISPs and their effort to expand broadband services and infrastructure. "…the combined number of fixed and mobile Internet connections increased from 50.2 million to 355.2 million from 2005 to 2015, and even as early as 2011 a substantial majority of Americans had access to broadband at home. As of 2016, roughly 91 percent of homes had access to networks offering 25 Mbps". (FCC, 2018a, p. 53). Although this number is impressive it's also misleading. The quoted number of 25 Mbps means that 91% of consumer *have* access to that level, however in a 2016 report by Akamai they found US consumers had an average connection of 10.2 Mbps. (2016, p. 18). Furthermore the FCC shows that 9% of homes are not able to connect to a broadband connection offering of 25 Mbps at all, which indicates that there is inequality in the system.

In 2015, under the *Title II,* ISPs were forced to treat all data equally under common carrier rules to ensure that all citizens can gain access to broadband services no matter where they are located in the US. Effectively telecommunication companies were legally obligated to extend services to all domiciles. By not holding ISPs to that same standard under the 2018 decision means that they aren't legally obligated to providing services to all US citizens. In 2015 the United States Census Bureau found that 77% of households in the United States had an internet subscription. (Ryan and Lewis, 2017, p. 4). The lack of internet connectivity can have a major effect on an individual as the Internet is used for information gathering, entertainment, communications, making purchases, banking, and health. (Fallows, 2004, p. i-v). "The responses of online Americans suggest that the Internet is a better tool for accomplishing some everyday activities than others. The Internet is most popular when its efficiency comes into play." (Fallows, 2004, p. iv). Having access to the Internet at home is crucial to an education as it can improve or help the learning experience. "It opens doorways to a wealth of information, knowledge and educational resources, increasing opportunities for learning in and beyond the classroom. Teachers use online materials to prepare lessons, and

students to extend their range of learning." (Internet Society, 2017, p. 1). To not have the same access denies the rights to underserved students to an equal education of those that better access.

Additionally, *Title II* forced ISPs to adopt standard rates. The report by the FCC states that "In theory, public utility regulation is intended to curb monopoly pricing just enough that the firm earns a rate of return on its investments equivalent to what it would earn in a competitive market. In practice, public utility regulation can depress profits below the competitive rate of return for a variety of reasons. This reduction in the expected return reduces the incentive to invest." (FCC, 2018a, p. 54). In terms of providing the best service possible, the idea of forcing regulations on ISPs could limit their ability to innovate, providing less access. According to the FCC (2018a), ISPs felt that the pressure of regulation harmed their ability to invest in the network and technology, whereas the previous light-touch framework worked better in that "…economic incentives, including competitive pressures, support Internet openness. We find that the gatekeeper theory, the bedrock of the *Title II Order*'s overall argument justifying its approach, is a poor fit for the broadband Internet access service market." (FCC, 2018a, p. 53) The FCC continued explaining why they thought regulations had a greater effect on ISPs and the Internet. "In theory, public utility regulation is intended to curb monopoly pricing just enough that the firm earns a rate of return on its investments equivalent to what it would earn in a competitive market. In practice, public utility regulation can depress profits below the competitive rate of return for a variety of reasons. This reduction in the expected return reduces the incentive to invest." (Ibid). The 2018 decision holds the idea that *Title II* regulation brought a level of uncertainty that has forced ISPs to withhold development and innovation within the industry. "…uncertainty regarding what is allowed and what is not allowed under the new Title II broadband regime has caused them to shelve projects that were in development, pursue fewer innovative business models and arrangements, or delay rolling out new features or services. Even large ISPs with significant resources have not been immune to the dampening effect that uncertainty can have on a firm's incentive to innovate." (FCC, 2018a, p. 58). The FCC cites the idea that regulation could pose an issue to innovation within Internet services, as they see similarities of regulation within the telecommunications industry. "Within the communications industry, it is apparent that the most regulated sectors, such as basic telephone service, have experienced the least innovation, whereas those sectors that have been traditionally free to innovate, such as Internet service, have greatly evolved." (FCC, 2018a, p. 59). ISPs are fearful of the idea of regulation due to the possibility that it could

quickly spiral out of control. This was highlighted by the decision as ISPs saw *Title II* highlighted short term goals, while leaving open ended opportunities create more in the future. "The record confirms that concern about 'regulatory creep'—whereby a regulator slowly increases its reach and the scope of its regulations—has exacerbated the regulatory uncertainty created by the *Title II Order*." (Ibid). However as Chairman Wheeler stated in a press conference in 2015, *Title II* was designed to ensure the industry does not create unreasonable interference of a user experience; acting as a test more or less. "No blocking, no throttling, no fast lanes. Those can be bright-line rules because we know about those issues. But we don't know where things go next. Using this kind of a construct of what is reasonable then we have created a playing field where there are known rules, and the FCC will sit there as a referee able to throw the flag." (C-SPAN, 2015). Wheeler mentions earlier in his statement that they don't know how the regulations would work in the long term, but does feel that the rules set would be more than enough to create stability. Still, the FCC felt that this wasn't enough of an assurance, leading to the new regulations. "With future regulations open to such uncertainties, Title II regulation adds a risk premium on each investment decision, which reduces the expected profitability of potential investments and deters investment." (FCC, 2018a, p. 60.) The key take away here is that ISPs want a clear understanding of the regulatory bounds that they can operate within, in order to best serve their customers and investors.

In *Restoring Internet Freedom,* the FCC notes that smaller ISPs and rural communities were affected to a greater extent by the *Title II* ruling. "…small ISPs and new entrants into the market face disproportionate costs and burdens as a result of regulation. Many small ISPs lack the extensive resources necessary to comply with burdensome regulation, and the record evinces a widespread consensus that reclassification of broadband Internet access service as a telecommunications service has harmed small ISPs by forcing them to divert significant resources to legal compliance and deterring them from taking financial risks." (FCC, 2018a, p. 61). Under *Title II Order,* regulation was seen to only harm citizens as it had affected the ability of smaller ISPs to operate, innovate, and expand. The new directive noted that these areas are known for having issues reaching similar national broadband standards, and that uncertainty under *Title II Order* which "…already has produced results that slow(ed) needed innovation and broadband adoption, effects that are most acutely felt in rural and socioeconomically-challenged urban communities." (FCC, 2018a, p. 62). Under *Title II* these smaller ISPs that service rural communities are forced to utilize fiscal resources to comply with regulation. "Many small ISPs lack the extensive

resources necessary to comply with burdensome regulation, and the record evinces a widespread consensus that reclassification of broadband Internet access service as a telecommunications service has harmed small ISPs by forcing them to divert significant resources to legal compliance and deterring them from taking financial risks." (FCC, 2018a, p. 61). This is clarified in subtext number 388 that compliance required economic resources to be diverted to legal counsel and outside consultancy to ensure that existing and planned services met the necessary requirements under the *Title II Order.* (FCC, 2018a, p. 61). Subtext number 387 also points out that if a small ISP were to not be in compliance with the *Title II Order,* it could be financially devastating to the company, and could harm the customers. (Ibid). Finally according to the FCC, under subtext number 391, they had found "…ISPs serving predominantly rural and underserved communities in Indiana, Arkansas, southwest Virginia, Washington State, northern Illinois and Missouri all curbed plans to expand high-speed Internet deployment, citing the *Title II Order* as their reasoning." (FCC, 2018a, p.62). Additionally it was reported by the Wireless Internet Service Providers Association (WISPA) who surveyed their members, found over 80% "…incurred additional expense in complying with the Title II rules, had delayed or reduced network expansion, had delayed or reduced services and had allocated budget to comply with the rules." (FCC, 2018a, p.63).

Under *Restoring Internet Freedom* the FCC is trying to assert that their actions of deregulation does provide more security for citizens by bringing broadband to areas that lack the services, in turn creating more security through connectivity to the Internet. Although it is unfortunate that *Title II* had created issues for smaller ISPs and rural communities, we must ask why larger ISPs weren't operating in these regions, especially if they have larger economic capacities. First we should understand that smaller ISPs work within rural or smaller communities due in part to larger ISPs not operating within those areas. These areas face less competition due to smaller ISPs having less capital to invest. Coincidentally the larger ISPs also generally don't work within these areas as the incurred costs to reach these areas are less profitable; if they invest in the building of infrastructure a smaller ISP would then be allowed to benefit. These areas are often referred as 'last-mile' services. "The general principle applicable to all contexts is that the last mile is the most difficult and expensive to build, but equally the most valuable: Dominating the last mile can provide a nearly unassailable competitive position. In telecom and other utilities, the cost of building the last mile is what results in natural monopolies, thereby requiring regulation." (Craig, 2017). Under *Title II* the FCC did state that there wouldn't be an unbundling of last-mile services by

ISPs. (Kastrenakes, 2015). Although this does mean that companies weren't able to patch out the last mile services to smaller ISPs vying for new business, it also means services provided by smaller ISPs might be less than what's provided by larger ISPs. However, the common carriage rules within *Title II* nullify the unbundling concern as the larger ISPs were supposed to provide Internet service in those areas, regardless of the cost to operate. Tom Wheeler stated "I have a facilities-based proclivity. I think if you're going to get competition, competition is a facilities-based issue, it is not an ersatz unbundling issue…" (Brodkin, 2016). In essence, this was supposed to create more competition as they imposed rules on unbundling of last-mile infrastructure to other businesses. "DSL Internet used to operate this way before the FCC under Republican leadership removed the unbundling requirement in 2005." (Ibid). ISPs that offered DSL would unbundle their services to smaller clients, which meant that upgrades to the system would be limited to the larger ISPs, essentially stagnating upgrades to the infrastructure and the eventual downfall of DSL. "DSL connections aren't easy to upgrade — especially over long distances. As a result, many large telecom firms decided that wireless broadband made a better target for their investments." (Pegoraro, 2016). Let's say that we set aside the issue of unbundling and allow for ISPs to parcel out their last-mile to smaller ISPs. Within *Restoring Internet Freedom* it does not explicitly determine that they would be opening up the practice of unbundling. Additionally if ISPs were this concerned for inaccessible communities to gain Internet access, then we should be seeing more action to resolve the issue. Which would mean that they would let smaller companies benefit from the work and investment they made to reach those areas, and possibly lose the chance for new customers.

When thinking about the decision of *Restoring Internet Freedom,* we can understand it as a reform on U.S. cybersecurity policy. While researching information an individual may find material pertaining to decisions and reasoning, and how it has effect on the security of individuals, businesses, and government. However what's not discussed about in the decision is how it affects the prospect of digital cybersecurity. According to the Electronic Frontier Foundation (EFF), they have identified five possible risk scenarios relating to the repeal of net-neutrality. These risks are in the form of traffic monitoring, encryption, ad media security loopholes, digital supercookies, and spyware. (Gillula and Eckersley, 2017).

In the case of traffic monitoring, ISPs are not disbarred from selling private browsing history. Additionally the FCC also removed previous rulings for the need to "…take reasonable measures to protect customer [personal information] from unauthorized use,

disclosure, or access…" (Brodkin, 2017c). This means that if ISPs are allowed to store and sell metadata. The risk to this is that if there was a security breach, hackers would have full access to an individual profile. "Imagine what could happen if hackers decided to target the treasure trove of personal information Internet providers start collecting. People's personal browsing history and records of their location could easily become the target of foreign hackers who want to embarrass or blackmail politicians or celebrities." (Gillula and Eckersley, 2017).

According to the EFF, the 2018 decision might have an effect on encrypted data and encryption technology. "Internet providers have proposed a standard (called Explicit Trusted Proxies) that would allow them to intercept your data, remove the encryption, read the data (and maybe even modify it), and then encrypt it again and send it on its way." (Gillula and Eckersley, 2017). If the ISPs are creating a profile on its users, individuals passing through their network, they could at some pint include the encrypted data as part of that persons profile. Additionally it could open up ISPs to treating encrypted data differently by placing a premium on customers who wish to have it remain encrypted. (Erlin, 2017). Moreover the process of de-encryption and re-encryption could be vulnerable to cyberattacks. (Gillula and Eckersley, 2017).

The last three points of concern by the EFF are separate issues, but could be considered under the same umbrella of operation. Ad media, digital supercookies, and spyware share the same issue of attackers gaining access to Internet users through system vulnerabilities. Ad media poses a risk when ISPs allow for ads to reflect a user search history; this requires a change in the coding of a site more rapidly, which could weaken the sites security codes in place. (Gillula and Eckersley, 2017). Sites like Google and Facebook may utilize cookies to track user history and interest by purchasing traffic history from an ISP, creating a profile for targeted ads. The EFF noted that there could be the possibility of supercookies developed by ISPs for every website that is visited, as practiced by Verizon, they could track every site visited even if the web browsers cookies were erased. (Ibid). Lastly it is feared that spyware that is pre-installed onto devices or in programs, by companies and ISPs, could be reprogrammed by a hacker to record personal data; if the attacker were able to override the spyware. "Thus, if hackers can find a vulnerability in the spyware, then they can use it as a sort of tunnel to get access to almost anything…" (Ibid).

However for all of these possible faults in security created by the 2018 decision, the American Enterprise Institute notes that it may provide security in protecting against Distributed Denial-of-Service (DDoS) attacks. "These attacks are a common method hackers

use to make Internet service inaccessible. Specifically, the attackers flood a specific open network system with large amounts of traffic to shut the systems down and create a temporary block to the target websites." (Tews, 2017). This would be beneficial to an ISP if an increase of traffic was detected, as the ISP would legally be able to slow or divert the traffic by throttling, disabling, or blocking that attack as it would fall under infrastructure maintenance or security protocols.

Although *Restoring Internet Freedom* was federally supported, mandating the alleviation of pressure by *Title II* on ISPs, there has been some push back to this move. Not only have citizens expressed their concerns via the FCC, elected officials and states have advocated for their constituents to create new net-neutrality measures. Republican Colorado Representative Mike Coffman submitted a congressional bill in July 2017, title *The 21st Century Internet Act.* This bill would hold a similar outline to that of the *Open Internet Order,* preventing ISPs from blocking, throttling, and prioritization. Additionally the bill would amend the *Telecommunications Act of 1934* by adding a new Title VIII. "This new classification would 'permanently codify into law the 'four corners' of net neutrality' by banning providers from controlling traffic quality and speed and forbidding them from participating in paid prioritization programs or charging access fees from edge providers…the legislation also makes it illegal for providers to participate in 'unfair or deceptive acts or practices'." (Kelly, 2018b). Additionally states have moved to keep the previous *Title II* in place, either constitutionally at the state-level or by executive powers of a state governor. Legislators in 30 states have introduced over 72 bills requiring various net neutrality principles, 13 states and the District of Columbia introduced 23 resolutions opposing the FCC, while 22 State Attorney Generals filed petitions against FCC in the U.S. Court of Appeals for the District of Columbia. (Dean, 2018). Currently the governors of Hawaii, New York, Montana, Rhode Island, and Vermont have all signed executive orders; the states of Oregon, Vermont, and Washington all officially have net-neutrality rules. (Ibid). Additionally the state of California has established their own set of net-neutrality laws as of late September 2018. (Lawler, 2018).

Although individual states have the right to create their own net-neutrality laws, it may be legally challenged by ISPs and the Federal government. The FCC decision, being a federal ruling, supersedes any State legislation due to Article VI, Clause 2 of the Constitution of the United States, stating that "…the Laws of the United States … shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the

Constitution or Laws of any State to the Contrary notwithstanding." (U.S. Const. amend. XI, cl. 2). Although the FCC and ISP have legal grounds to implement the 2018 decision, States having their own rulings shows that there is a consensus of concern over the FCCs decision to dismantle net-neutrality. An individual states obligation is to protect the needs of its constituents. Federally, laws are passed with the interest of supporting the whole population of the United States. To have eight states and one district, a quarter of the US population, disagree with a federal ruling should make a government pause and check if the ruling is meeting the needs of the people.

7. Discussion on the US Governance

To understand the FCCs 2018 decision, we should ask whether the United States is a regulatory state or modern welfare state. We will then be able to comprehend the actions behind their decision.

A modern welfare state is generally aims to "…implement social policies to remedy the suffering caused by ruthless market mechanisms. They provide insurances to allow citizens to prepare for the vicissitudes of life, such as aging, illness, injuries, retirement, and unemployment." (Lee and Koo, 2017). The problem with this definition is that if any state has a form of social programs they too could be considered a welfare state by that virtue. However the welfare state can be differentiated between two aspects, welfare sector and welfare politics. A welfare sector pertains to "…a range of social services or social institutions…", while welfare politics pertain to "…patterns of political action based on welfare-related normative orientations." (Leisering, 2003, p. 179). What this means is that a welfare state is one where the actions of a politician is prioritized on the need to provide security of their citizens. According to Harry Girvetz (cited in Leisering 2003) "Such a state emerges when a society or its decision-making groups become convinced that the welfare of the individual . . . is too important to be left to custom or to informal arrangements and private understandings and is therefore a concern of government." (Ibid). Based on the proceedings of the FCC and the actions of the United States, we can say that it meets the minimum requirements of a welfare state, placing concern for its citizens secondary to that of the needs of the government. If the FCC was more concerned for the citizens then we would have seen tighter control of ISPs in order to provide protections; similar to that of France or Norway.

This would mean that the US aligns more so as a regulatory state. According to Michael Moran, he believes that the US is a regulatory state as "Americans virtually invented the modern regulatory state, in the sense that the United States was the great pioneer of the administrative technology of controlling business through law-backed specialized agencies rather than through the technique of public ownership." (Moran, 2002, p. 392). For a liberalized state like the US, a regulatory practice is the result of competing private interests to protect commodities, and non-commodities. The ideal regulation would have adverse conditions amongst an industry, where entities voluntarily comply under norms to control the system, while keeping constant dialogue between regulators and regulated. (Moran, 2002, p. 398). However currently the US practices a command style regulation places where demands are placed on industries primarily to conform to the needs of the government. When the FCC handed down the net neutrality ruling, it was the government imposing rules that they felt the industry needed to be healthy. However when command regulation causes stress on an industry, public policymakers may respond by deregulating those industries. (Moran, 2002,p. 397). Thus the issue of command regulation isn't viewed as just providing incorrect policies, rather they are perceived as the problem altogether. To deregulate would mean the imposition of self-regulation on the industry. (Ibid). Although self-regulation can be useful for the industry, problems arise when the interests within industries become opportunistic. An example of this would be the FCC asking ISPs to self-report under *Restoring Internet Freedom.* This is why a state may impose some form of regulation at a minimum level. Even though the FCC effectively de-regulated ISPs and imposed self-regulation, they still asked to ISPs to comply with some regulations and to report to the FTC. From this we can entertain the idea that the 2018 *Restoring Internet Freedom* was written from the perspective of a regulatory state.

Although the US government practices a regulatory governance framework to provide security to citizens, an emancipatory practice in my view would follow a welfare state framework. The goals of a welfare state are similar to that of emancipation as its goal relates to "…the freeing of individuals from arbitrary structures that prevent them from living as they would wish." (McDonald, 2012). This is important to realize when implementing it as a tool for analysis. Although a regulatory state has different concern, referent object, we can still apply emancipatory practices as a thought tool. A regulatory state that investigates a security risk may still ask 'who are we securing?', 'from what threats?', and 'by what means?'(McDonald, 2012). Although the FCC focused on businesses as their primary

referent object, it can't go unnoticed that there was a human factor as a concern. The difference is the final choice the FCC may be different than what was made under a welfare state.

8. Conclusion

In this thesis I have presented information on the 2018 decision to remove net-neutrality rules and regulatory standards of ISPs by the FCC, as per instructions of *Restoring Internet Freedom.* The goal of this policy had three main goals. First, "…end utility style regulation of the Internet in favor of the market-based policies necessary to preserve the future of Internet freedom." (FCC, 2018a, p. 2). Second, it reinstates bright-line rules, and requires ISPs to be transparent. "Disclosure of network management practices, performance, and commercial terms of service is important for Internet freedom because it helps consumers choose what works best for them and enables entrepreneurs and other small businesses to get technical information needed to innovate. Individual consumers, not the government, decide what Internet access service best meets their individualized needs." (FCC, 2018a, p. 3). Third, the elimination of *Title II* conduct rules. "Lastly, we find that the conduct rules are unnecessary because the transparency requirement we adopt, together with antitrust and consumer protection laws, ensures that consumers have means to take remedial action if an ISP engages in behavior inconsistent with an open Internet." (FCC, 2018a, p.3).

The FCCs decision was based on information and testimony that was provided by businesses, large and small ISPs, non-profits, and citizens. The final decision was made by the five board members upon review of the gathered information, by a 3-2 vote. We can say that the decision was of a regulatory governance style as the FCC had a greater concern for the broadband industry, while citizen concerns were considered secondary. The board conducted their business similarly to that of a multistakeholder governance model. Where "…two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules." (Raymond and DeNardis, 2015, p. 574). However, a caveat to this is that the FCC doesn't practice a true multistakeholder model, as the board made the final decision. Still, the board is made of members that must weigh the interests of all the contributing parties.

Based on my case study I asked: *How is the governing of internet access in the United States, as expressed in the new 2018 ruling, affecting citizens' security?* Through my research

I saw the new rule potentially as a negative effect on an individual's ability to have security while using or accessing the internet.

Within the decision by the FCC they had to decide the best course of action to provide the Internet security of citizens of the United States. In the three main goals for *Restoring Internet Freedom*, they explicitly focus on the practices of the FCC and how they relate to the welfare of ISPs. Specifically they address that the 2018 decision was designed to maintain and protect a competitive free market, and reject government control of the Internet. (FCC, 2018a, p. 2). ISPs felt that the heavy handed regulations made it difficult for them to operate and provide the best services to customers. (Brogan, 2017). Comparatively, the 2015 *Title II Order* placed more emphasis on the support and security needs of the citizens and consumers. (FCC, 2015, p. 7). Considering during the bright-line regulations that existed prior to 2015 saw companies practice throttling, capping, blocking, and creating a tiered system. (Mitchell, 2017). Additionally, the large ISPs unwillingness to develop new infrastructure also shows that the profit took precedence over the welfare of their customers and US citizens. (Malone, 2017). Under the 2015 ruling, the FCC had the power to address anti-competitiveness of ISPs, as well as regulating their actions. (Falcon, 2017). While under the 2018, ISPs are asked to self-regulate, with the ill-equipped FTC providing oversight. (Ibid). From these examples, we can see that the FCC is choosing to de-regulate in order to provide ISPs a greater economic security. However this comes at a price to citizens as the ISPs are asked to self-regulate in an industry where they have historically been known to work against citizens.

The FCC mentions that the net neutrality measures imposed under *Title II* made it difficult for ISPs to operate and invest in infrastructure. However upon further analysis, the years during *Title II* had an average increase in investments and expenditures over previous years. (Brogan, 2017). Although there was a large increase of new users of broadband from 2005-2015, by 2016, there was a large population that was still underserved and meeting subpar internet connection speeds. (Akamai, 2016). Not having quality access to the Internet does create a sense of inequality, as education and daily life revolves around access to the Internet. (Internet Society, 2017, p. 1). Part of this problem was a result of ISPs avoiding new infrastructure and not adopting standard rates, this had a major effect on poor and rural community access the internet.(Malone, 2017). Under *Title II* it was required for ISPs to meet the needs of those customers despite the cost it would take to invest in the area, as it was protected by Common Carriage laws. (Brodkin, 2016). Lastly we must consider the viewpoint of the citizen, where 22 million individuals voiced their opinion but were left out of the decision fearing it was a DDoS attack; unfortunately this was a lie. (Brodkin, 2018).

Additionally nine states enacted their own net-neutrality laws, covering 25% of the US population. (Dean, 2018). These states also provide agency for individuals, lending a greater influence on state matters; in this case the citizens have a definite reservation toward *Restoring Internet Freedom.*

The emancipatory practice asks 'who are we securing?', 'from what threats?', and 'by what means?' (McDonald, 2012). Within this mode of thought we must recognize the state as an institution is designed to be viewed "…as *possible* agents for security: means for advancing the wellbeing of their own citizens." (Ibid). From the perspective of Security as Emancipation we should be framing the research around how it affects individuals, instead the FCC took a stance on how *Restoring Internet Freedom* would affect businesses. This concern for businesses show that individuals would of less importance. The threat that the FCC was concerned about is how restrictive regulations protecting customers were threatening the ability for ISPs to operate. The FCC seemed to show little concern for the security of citizens. Even when there are clear examples of ISPs infringing the rights of citizens, it's expected that the ISPs will be able to deliver better security from the market over government regulations. How the FCC eliminated the threat of restrictive regulations to ISPs came from the elimination of net neutrality rules. In return they ask ISPs to be open about their practices to treat customers fairly, and to work with the FTC. This implies implicit trust in ISPs to actually be open. However, I must add that as the ruling is still in its infancy, ISPs are being heavily scrutinized by the government, academics, organizations, and citizens; which could affect how ISPs operate. Despite the trust in the market to deliver security over the government, with minimal protections, may prove an issue at a later date. Based on the study, analysis, and summary of my case, this is how I came to the conclusion that the FCCs *Restoring Internet Freedom* of 2018 may have the potential to be a negative effect on an individual's ability to have security while using or accessing the internet.

Bibliography

47 C.F.R. § 8.9(b)

47 U.S.C. § 151

47 U.S.C. § 153(24)

47 U.S.C. § 153(50)

47 U.S.C. § 153(53)

476 U.S. 355

Ablon, L. (2018). Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. [ebook] Santa Monica: RAND Corporation. Available at: https://www.rand.org/pubs/testimonies/CT490.html [Accessed 25 Oct. 2018].

Akamai (2016). *Akamai's - State of the Internet*. Q2 2016 Report. [online] Cambridge: Akamai. Available at: https://www.akamai.com/us/en/multimedia/documents/state-of-the-Internet/akamai-state-of-the-Internet-connectivity-report-q2-2016.pdf [Accessed 10 Jun. 2018].

Altheide, D., and Schneider, C. (2013). *Qualitative Media Analysis* (2nd ed., Vol. Volume 38, Qualitative research methods). Los Angeles, Calif: Sage.

Anderson, J. and Rainie, L. (2018). *Stories From Experts About the Impact of Digital Life*. [online] Pew Research Center: Internet, Science & Tech. Available at: http://www.pewInternet.org/2018/07/03/the-positives-of-digital-life/ [Accessed 24 Oct. 2018].

Anderson, M., Perrin, A., and Jiang, J. (2018). *11% of Americans don't use the internet. Who are they?* [online] Available at: http://www.pewresearch.org/fact-tank/2018/03/05/some-americans-dont-use-the-internet-who-are-they/ [Accessed 8 Dec. 2018].

Becker, G., Carlton, D. and Sider, H. (2010). Net Neutrality and Consumer Welfare. *Journal of Competition Law and Economics*, 6(3), pp.497-519.

Beede, D. (2014). *Competition Among U.S. Broadband Service Providers*. OCE Issue Brief: #01-14. Washington, D.C.: U.S. Department of Commerce: Economics and Statistics Administration.

Benedek, W., Bauer, V. and Kettemann, M. (2008). *Internet Governance and the Information Society: Global Perspectives and European Dimensions*. Utrecht, the Netherlands: Eleven International Pub.

Bettilyon, T. (2017). *Network Neutrality: A History of Common Carrier Laws 1884–2018.* [online] Medium. Available at:

https://medium.com/@TebbaVonMathenstien/network-neutrality-a-history-of-common-carrier-laws-1884-2018-2b592f22ed2e [Accessed 8 Jun. 2018].

Booth, K. (1991). *Security and Emancipation*. Review of International Studies, 17(04), pp.313-326.

Brodkin, J. (2016). *Why Tom Wheeler rejected broadband price caps and last-mile unbundling*. [online] Ars Technica. Available at: https://arstechnica.com/information-technology/2016/03/why-tom-wheeler-rejected-broadband-price-caps-and-last-mile-unbundling/ [Accessed 9 Nov. 2018].

Brodkin, J. (2017a). *Verizon accused of throttling Netflix and YouTube, admits to "video optimization"*. [online] Ars Technica. Available at: https://arstechnica.com/information-technology/2017/07/verizon-wireless-apparently-throttles-streaming-video-to-10mbps/ [Accessed 6 Apr. 2018].

Brodkin, J. (2017b). *Verizon accused of throttling Netflix and YouTube, admits to "video optimization"*. [online] Ars Technica. Available at: https://arstechnica.com/information-technology/2017/07/verizon-wireless-apparently-throttles-streaming-video-to-10mbps/ [Accessed 6 Apr. 2018]. *Tom Wheeler defends Title II rules, accuses Pai of helping monopolists*. [online] Ars Technica. Available at: https://arstechnica.com/tech-policy/2017/06/tom-wheeler-defends-title-ii-rules-accuses-pai-of-helping-monopolists/ [Accessed 14 Mar. 2018].

Brodkin, J. (2017c). *FCC to halt rule that protects your private data from security breaches*. [online] Ars Technica. Available at: https://arstechnica.com/tech-policy/2017/02/isps-wont-have-to-follow-new-rule-that-protects-your-data-from-theft/ [Accessed 9 Nov. 2018].

Brodkin, J. (2018). *FCC lied to Congress about made-up DDoS attack, investigation found*. [online] Ars Technica. Available at: https://arstechnica.com/tech-policy/2018/08/fcc-lied-to-congress-about-made-up-ddos-attack-investigation-found/ [Accessed 9 Nov. 2018].

Brogan, P. (2017). *Broadband Investment Continues Trending Down in 2016*. [online] Washington, D.C.: USTelecom. Available at: https://www.ustelecom.org/sites/default/files/documents/Broadband%20Investment%20Trending%20Down%20in%202016.pdf [Accessed 3. 2018].

Brotman, S. (2016). *Was the 1996 Telecommunications Act successful in promoting competition?*. [online] Brookings Institute. Available at: https://www.brookings.edu/blog/techtank/2016/02/08/was-the-1996-telecommunications-act-successful-in-promoting-competition/ [Accessed 6 Dec. 2018].

Buzan, B. and Hansen, L. (2009). *The Evolution of International Security Studies*. 9th ed. Cambridge: Cambridge University Press.

Cannon, R., (2002). *The Legacy of the Federal Communications Commission's Computer Inquiries*. Fed. Comm. LJ, *55*.

CERIAS. (2018). *CERIAS - Broadband vs. Dialup Internet Connection*. [online] CERIAS Available at: https://www.cerias.purdue.edu/site/education/k-12/cerias_resources/files/infosec_newsletters/06broadband.php [Accessed 1 Jun. 2018].

Choucri, N. and Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*, 68(2), pp.70-77.

Clark, D., Berson, T. and Lin, H. (2014). *At the nexus of cybersecurity and public policy*. Washington, District of Columbia: The National Academies Press.

Clough, J. (2014). *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation.* Monash University Law Review 40(3): 698-736.

Coldewey, D. (2018). *FCC report keeps faster definition of broadband and separates mobile from fixed connections*. [online] TechCrunch. Available at: https://techcrunch.com/2018/01/18/fcc-report-keeps-faster-definition-of-broadband-and-separates-mobile-from-fixed-connections/ [Accessed 7 Dec. 2018].

Cornell Law School. (2018). *Bright-Line Rule – Definition.* [online] Cornell Law School: Legal Information Institute. Available at: https://www.law.cornell.edu/wex/bright-line_rule [Accessed: 03 Mar. 2018].

Craig, R. (2017). *The 'last mile' in education and training*. [online] TechCrunch. Available at: https://techcrunch.com/2017/06/25/the-last-mile-in-education-and-training/ [Accessed 9 Nov. 2018].

C-SPAN. (2015). *Statement of Tom Wheeler, Former Chairman, FCC, Press Conference (Feb. 26, 2015)*. [online] C-SPAN.org. Available at: https://www.cspan.org/video/?c4534447/wheeler-general-conduct-standard. [Accessed 5 Nov. 2018]

Davidson, J. (2015). *AT&T Just Showed Us the Only Way We'll Get Better Internet Service*. Time.com. http://time.com/money/3712151/att-google-competition-Internet/ [Accessed 4 Apr. 2018].

de Bossey, C. (2005). *Report of the Working Group on Internet Governance*. [online] WGIG. Available at: http://akgul.bilkent.edu.tr/DNS/WGIGREPORT.pdf. [Accessed: 30 Sept. 2018].

Dean, D. (2018). *Net Neutrality Legislation in States*. [online] NCSL.org. Available at: http://www.ncsl.org/research/telecommunications-and-information-technology/net-neutrality-legislation-in-states.aspx [Accessed 9 Nov. 2018].

DeNardis, L. and Raymond, M., (2013). *Thinking Clearly About Multistakeholder Internet Governance.* Eighth Annual GigaNet Symposium. Bali, Indonesia.

Encyclopedia Britannica. (2018). *Internet service provider (ISP).* [online] brittanica.com Available at: https://www.britannica.com/technology/Internet-service-provider [Accessed 1 Jun. 2018].

Erlin, T. (2017). *The Security Implications of Killing Net Neutrality*. [online] Tripwire.com. Available at: https://www.tripwire.com/state-of-security/featured/security-implications-killing-net-neutrality/ [Accessed 9 Nov. 2018].

European Union Agency for Network and Information Security (2016). *Definition of Cybersecurity - Gaps and overlaps in standardisation*. [PDF] Athens: European Union Agency for Network and Information Security. Available at: https://www.enisa.europa.eu/publications/definition-of-cybersecurity [Accessed 11 May 2018].

Falcon, E. (2017). *More than 40 ISPs Across the Country Tell Chairman Pai to Not Repeal Network Neutrality and Maintain Title II Enforcement*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2017/06/isps-across-country-tell-chairman-pai-not-repeal-network-neutrality [Accessed 11 Apr. 2018].

Fallows, D. (2004). *The Internet and Daily Life*. Washington, D.C.: Pew Internet & American Life Project.

Federal Telecommunications Standards Committee. (1996). *Federal Standard 1037C: Glossary of Telecommunications Terms (FED-STD-1037C).* Pages T: 4-5. National Communications System Technology Program Office, Arlington, Virginia.

Federal Communications Commission. (2009). *NPRM: Preserving the Open Internet Broadband Industry Practices.* Washington, D.C.: Federal Communications Commission.

Federal Communications Commission (2014). *Protecting and Promoting the Open Internet NPRM*. Washington, D.C.: Federal Communications Commission.

Federal Communications Commission, (2015). *In the matter of protecting and promoting the open Internet.* Washington, D.C.: Federal Communications Commission.

Federal Communications Commission. (2017). *FCC Initiative – Restoring Internet Freedom.* [online] FCC. Available at: https://www.fcc.gov/restoring-Internet-freedom [Accessed: 03 Mar. 2018].

Federal Communications Commission (2018a). *DECLARATORY RULING, REPORT AND ORDER, AND ORDER: Restoring Internet Freedom*. Washington, D.C.: Federal Communications Commission.

Federal Communications Commission. (2018b). *About the FCC*. [online] FCC. Available at: https://www.fcc.gov/about/overview [Accessed 9 Nov. 2018].

Finley, K. (2018) *The Wired Guide to Net Neutrality.* [online] Wired. Available at: https://www.wired.com/story/guide-net-neutrality/ [Accessed 15 May 2018]

Fisher, T. (2017). *"What Is Bandwidth Throttling?"* [online] Lifewire.com. Available at: https://www.lifewire.com/what-is-bandwidth-throttling-2625808 [Accessed 03 Mar. 2018].

Future State Podcast. (2018). *The Future State with Richard A. Clarke - About*. [online] Available at: https://www.futurestatepodcast.com/ [Accessed 4 Nov. 2018].

Garcia, S., and Palhares, A. (2013). Reflections on Virtual to Real: Modern Technique, International Security Studies and Cyber Security Environment. In: J. Kremer and B. Müller, ed., *Cyberspace and International Relations: Theory, Prospects and Challenges*. Berlin: Springer.

Gellman, R. (2016). *Can Consumers Trust the FTC to Protect Their Privacy?*. [online] American Civil Liberties Union. Available at: https://www.aclu.org/blog/privacy-technology/Internet-privacy/can-consumers-trust-ftc-protect-their-privacy [Accessed 6 Mar. 2018].

Gillula, J. and Eckersley, P. (2017). *Five Ways Cybersecurity Will Suffer If Congress Repeals the FCC Privacy Rules*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/deeplinks/2017/03/five-ways-cybersecurity-will-suffer-if-congress-repeals-fcc-privacy-rules [Accessed 9 Nov. 2018].

Golafshani, N. (2003). *Understanding Reliability and Validity in Qualitative Research*. The Qualitative Report, 8(4), pp.597-606.

Goncharenko, R. (2018). *Russia moves toward creation of an independent Internet | DW | 17.01.2018*. [online] Deutsche Welle. Available at: https://www.dw.com/en/russia-moves-toward-creation-of-an-independent-Internet/a-42172902 [Accessed 9 Nov. 2018].

Good Harbor Cyber Security Risk Management. (2018). *Who We Are*. [online] Available at: https://www.goodharbor.net/ [Accessed 4 Nov. 2018].

Governmental Advisory Committee (2007). *GAC Principles Regarding New gTLDs*. Los Angeles: Governmental Advisory Committee.

Grandoni, D. (2012). *21 YEARS LATER: World's First Website Still Online*. [online] HuffPost UK. Available at: https://www.huffingtonpost.com/2012/08/06/worlds-first-website_n_1747476.html [Accessed 9 Nov. 2018].

Hansell, S. (2005). *Cable Wins Internet-Access Ruling*. [online] Nytimes.com. Available at: https://www.nytimes.com/2005/06/28/technology/cable-wins-Internetaccess-ruling.html [Accessed 6 Mar. 2018].

Hansen, L. and Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53(4), pp.1155-1175.

Harvard Law Review. (2016). *FTC v. Wyndham Worldwide Corp.* [online] Harvard Law. Available at: https://harvardlawreview.org/2016/02/ftc-v-wyndham-worldwide-corp/ [Accessed 5 Mar. 2018].

Hitlin, P., Olmstead, K. and Toor, S. (2017). *Public Comments to the Federal Communications Commission About Net Neutrality Contain Many Inaccuracies and Duplicates*. [online] Pew Research Center. Available at: http://www.pewInternet.org/2017/11/29/public-comments-to-the-federal-communications-commission-about-net-neutrality-contain-many-inaccuracies-and-duplicates/ [Accessed 1 Aug. 2018].

Hofmann, J. (2016). Multi-stakeholderism in Internet governance: putting a fiction into practice. *Journal of Cyber Policy*, 1(1), pp.29-49.

Holmes, A., Fox, E., Wieder, B. and Zubak-Skees, C. (2016). *Rich people have access to high-speed Internet; many poor people still don't*. [online] Center for Public Integrity. Available at: https://www.publicintegrity.org/2016/05/12/19659/rich-people-have-access-high-speed-Internet-many-poor-people-still-dont [Accessed 11 Apr. 2018].

IANA (2018). *IANA — About us*. [online] IANA. Available at: https://www.iana.org/about [Accessed 10 Nov. 2018].

Ignatius, D. (2018). *Working with Russia on cybercrime is like hiring a burglar to protect the family jewels*. [online] washingtonpost.com. Available at: https://www.washingtonpost.com/opinions/global-opinions/working-with-russia-on-cyber-regulation-is-like-paying-a-bully-for-protection/2018/09/04/b16787ea-b08e-11e8-9a6a-565d92a3585d_story.html?utm_term=.4eb912804bb9 [Accessed 6 Nov. 2018].

Inc.com. (2018). *Internet Service Providers (ISPs)*. [online] Inc.com. Available at: https://www.inc.com/encyclopedia/Internet-service-providers-isps.html [Accessed 1 Jun. 2018].

Internal Revenue Service. (2018). *Exemption Requirements Section 501(c)(3) Organizations.* [online] Available at: https://www.irs.gov/charities-non-profits/charitable-organizations/exemption-requirements-section-501c3-organizations [Accessed 4 Dec. 2018].

International Telecommunication Union. (2018). *Statistics*. [online] Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx [Accessed 8 Dec. 2018].

Internet Governance Forum Secretariat (2006). *The Internet Governance Forum (IGF) Inaugural Meeting - Background Report*. Athens, 30 October - 2 November 2006. Geneva: Internet Governance Forum.

Internet Society. (2015). *Internet Governance: An Internet Society Public Policy Briefing.* [ebook] Geneva: Internet Society. Available at: https://www.Internetsociety.org/wp-content/uploads/2017/09/ISOC-PolicyBrief-InternetGovernance-20151030-nb.pdf [Accessed 1 Oct. 2018].

Internet Society. (2017). *Internet Access and Education: Key considerations for policy makers.* Geneva: Internet Society.

Jones, R. W. (2000). *Security, Strategy, and Critical Theory*. [online] The American Political Science Review. Available at: https://www.researchgate.net/publication/265023798_Security_Strategy_and_Critical_Theory 94.10.2307/2586105

Justia Law. (2018). *United States Telecom Assoc. v. FCC, No. 15-1063 (D.C. Cir. 2016).* [online] Justia Law. Available at: https://law.justia.com/cases/federal/appellate-courts/cadc/15-1063/15-1063-2016-06-14.html [Accessed 16 Apr. 2018].

Kastrenakes, J. (2015). *These are the FCC's full rules for protecting net neutrality.* [online] The Verge. Available at: https://www.theverge.com/2015/3/12/8116237/net-neutrality-rules-open-Internet-order-released [Accessed 4 Apr. 2018].

Kastrenakes, J. (2017). *FCC extends net neutrality comment period by two weeks*. [online] The Verge. Available at: https://www.theverge.com/2017/8/11/16135708/fcc-net-neutrality-comment-period-extended-two-weeks [Accessed 10 Apr. 2018].

Kohlbacher, F. (2006). *The Use of Qualitative Content Analysis in Case Study Research.* Forum: Qualitative Social Research, 7(1), p. Art. 21. Available at: http://www.qualitative-research.net/index.php/fqs/article/view/75/153 [Accessed 15 Jan. 2018]

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, 38(2), pp.7-40.

Kelly, M. (2018a). *Investigation proves there was no cyberattack on the FCC prior to net neutrality ruling*. [online] The Verge. Available at: https://www.theverge.com/2018/8/7/17661594/fcc-investigation-cyberattack-ajit-pai-net-neutrality-ddos [Accessed 9 Nov. 2018].

Kelly, M. (2018b). *GOP congressman introduces bill to reinstate net neutrality rules*. [online] The Verge. Available at: https://www.theverge.com/2018/7/17/17577490/net-neutrality-republican-congress-bill-mike-coffman [Accessed 9 Nov. 2018].

Kranz, M. (2018). *6 ways the Internet of Things is improving our lives*. [online] World Economic Forum. Available at: https://www.weforum.org/agenda/2018/01/6-ways-the-Internet-of-things-is-improving-our-lives/ [Accessed 24 Oct. 2018].

Lak, M. (2009). *Governance in the International Security Arena: A Role for Non-State Stakeholders as Co-providers of Security*. [ebook] The Hague: Clingendael Institute. Available at: https://www.clingendael.org/sites/default/files/pdfs/20091000_cscp_paper_lak_governance.pdf [Accessed 30 Sep. 2018].

Lawler, R. (2018). *CA governor signs net neutrality bill into law, Justice Department sues*. [online] Engadget. Available at: https://www.engadget.com/2018/09/30/net-neutrality-california-brown-sb-822/ [Accessed 9 Nov. 2018].

Lecher, C. (2017). *FCC says its comment system was hit by denial-of-service attacks*. [online] The Verge. Available at: https://www.theverge.com/2017/5/8/15583406/fcc-ddos-net-neutrality-john-oliver [Accessed 11 Apr. 2018].

Lee, C. and Koo, I. (2017). The Welfare States and Poverty. *Oxford Handbooks Online*.

Lee, T. (2013). *How a grad student trying to build the first botnet brought the Internet to its knees*. [online] washingtonpost.com. Available at: https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/?utm_term=.26ad2fb17edb [Accessed 8 Nov. 2018].

Leiner, B., Cerf, V., Clark, D., Kahn, R., Kleinrock, L., Lynch, D., Postel, J., Roberts, L. and Wolff, S. (1997). *Brief History of the Internet*. Reston: Internet Society.

Leisering, L. (2003). Nation State and Welfare State: An Intellectual and Political History. *Journal of European Social Policy*, 13(2), pp.175-185.

Lucchesi, N. (2018). *FCC Chair Ajit Pai Reveals Why He Couldn't Talk About Net Neutrality "Hack"*. [online] Inverse. Available at: https://www.inverse.com/article/48136-fcc-chair-ajit-pai-reveals-why-he-couldn-t-talk-about-net-neutrality-hack [Accessed 9 Nov. 2018].

Malone, C. (2017). *The Worst Internet In America*. [online] FiveThirtyEight. Available at: https://fivethirtyeight.com/features/the-worst-Internet-in-america/ [Accessed 8 Apr. 2018].

Marcon, M., Dischinger, M., Gummadi, K. and Vahdat, A. (2011). *The local and global effects of traffic shaping in the Internet.* 2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011).

Mahtesian, C. and Shafer, J. (2018). *Where's the U.S. doctrine on cyber warfare?*. [online] POLITICO. Available at: https://www.politico.com/newsletters/morning-cybersecurity/2018/03/13/wheres-the-us-doctrine-on-cyber-warfare-129860 [Accessed 4 Nov. 2018].

Masters, J. (2014). *What Is Internet Governance?* [online] Council on Foreign Relations. Available at: https://www.cfr.org/backgrounder/what-Internet-governance [Accessed 16 Aug. 2018].

Maurer, T. and Ebert, H. (2017). International Relations and Cyber Security: Carnegie Contribution to Oxford Bibliographies. [online] Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2017/01/11/international-relations-and-cyber-security-carnegie-contribution-to-oxford-bibliographies-pub-67672 [Accessed 13 Jun. 2018].

McDonald, M. (2012). *Security, the Environment and Emancipation*, 1st Edition. [ebook]. Retrieved from https://online.vitalsource.com/#/books/9781136645952/

Mitchell, C. (2017). *Repealing Net Neutrality Puts 177 Million Americans at Risk.* [online] Institute for Local Self-Reliance. Available at: https://muninetworks.org/content/177-million-americans-harmed-net-neutrality [Accessed: 04 Apr. 2018]

MORAN, M. (2002). Review Article: Understanding the Regulatory State. *British Journal of Political Science*, 32(02), pp.391-413.

Nakashima, E. (2015). *Hacks of OPM databases compromised 22.1 million people, federal authorities say*. [online] washingtonpost.com. Available at: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.7e68c607444c [Accessed 9 Nov. 2018].

Norwegian Communications Authority. (2017). *Net neutrality in Norway*. [online] Available at: https://eng.nkom.no/technical/internet/net-neutrality/net-neutrality-in-norway [Accessed 6 Dec. 2018].

NYC Mayor's Office of the Chief Technology Officer (2018). *Truth in Broadband: Access and Connectivity in New York City*. New York: City of New York.

Nye, J.S. (2010). *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs.

Nye, J.S. (2011). Nuclear lessons for cyber security?. *Strategic Studies Quarterly*, *5*(4), pp.18-38.

OECD (2006). *Evolution in the Management of Country Code Top-Level Domain Names (ccTLDs)*. Paris: Organisation for Economic Co-operation and Development.

O'Flaherty, K. (2018). *Cyber Warfare: The Threat From Nation States*. [online] Forbes. Available at: https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/ [Accessed 4 Nov. 2018].

Patrick, S. (2014). *Brazil's Internet Summit: Building Bridges to Avoid "SplInternet"*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/blog/brazils-Internet-summit-building-bridges-avoid-splInternet#more-3748 [Accessed 16 Aug. 2018].

PC Mag. (2018). *Bandwidth Throttling Definition*. [online] PC Mag. Available at: https://www.pcmag.com/encyclopedia/term/67561/bandwidth-throttling [Accessed 26 Jul. 2018].

Pegoraro, R. (2016). *FCC study shows DSL is terrible, but it doesn't have to be*. [online] Finance.yahoo.com. Available at: https://finance.yahoo.com/news/dsl-too-slow-fcc-190606412.html?guccounter=1 [Accessed 9 Nov. 2018].

Pegoraro, R. (2017). *The Trump administration gets the history of Internet regulations all wrong*. [online] Washington Post. Available at: https://www.washingtonpost.com/posteverything/wp/2017/05/12/the-trump-

administration-gets-the-history-of-Internet-regulations-all-wrong/?noredirect=on&utm_term=.da5be433f01a [Accessed 12 Apr. 2018].

Post, D. (2014). *Does the FCC really not get it about the Internet?* [online] Washington Post. Available at: https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/10/31/does-the-fcc-really-not-get-it-about-the-Internet/?utm_term=.369e1a626b58 [Accessed 1 June 2018].

Otero, V. (2017). *The Chart, Version 3.0: What, Exactly, Are We Reading?*. [online] Ad Fontes Media. Available at: http://www.adfontesmedia.com/the-chart-version-3-0-what-exactly-are-we-reading/ [Accessed 1 Dec. 2018].

Radu, R. (2013). Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace. In: J. Kremer and B. Müller, ed., *Cyberspace and International Relations: Theory, Prospects and Challenges*. Berlin: Springer.

Raymond, M. and DeNardis, L. (2015). Multistakeholderism: anatomy of an inchoate global institution. *International Theory*, 7(03), pp.572-616.

Reardon, R. and Choucri, N. (2012) *The Role of Cyberspace in International Relations: A View of the Literature*. Paper presented at the 2012 ISA Annual Convention, San Diego, CA. April 1, 2012.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), pp.5-32.

Root-servers.org. (2018). *Root Server Technical Operations Assn*. [online] Available at: http://www.root-servers.org/ [Accessed 5 Dec. 2018].

Rizzo, S. (2018). *Will the FCC's net neutrality repeal grind the Internet to a halt?*. [online] washingtonpost.com. Available at: https://www.washingtonpost.com/news/fact-checker/wp/2018/03/05/will-the-fccs-net-neutrality-repeal-grind-the-internet-to-a-halt/?utm_term=.b8ae7c97bcf1 [Accessed 5 Dec. 2018].

Rouse, M. (2018). *Bright Line Rule – Definition.* [online] WhatIs.com. Available at: https://whatis.techtarget.com/definition/bright-line-rule [Accessed: 03 Mar. 2018]

Ryan, C. and Lewis, J. (2017). *Computer and Internet Use in the United States: 2015*. Washington, D.C.: United States Census Bureau.

Savov, V. (2018). *The US net neutrality fight affects the whole world*. [online] The Verge. Available at: https://www.theverge.com/2017/11/23/16693840/net-neutrality-us-fcc-global-effect [Accessed 15 Nov. 2018].

Shepardson, D. (2017). *U.S. agency prepares to hand over Internet oversight to FTC*. [online] Reuters. Available at: https://www.reuters.com/article/us-usa-Internet/u-s-agency-prepares-to-hand-over-Internet-oversight-to-ftc-idUSKBN1E52N9 [Accessed 21 Mar. 2018].

Shepherd, L. J. (2013). *Critical Approaches to Security: An introduction to theories and methods*. 1st ed. London: Routledge.

Shim, E. (2014). *How Politically Biased Is Each Industry? Check These Charts*. [online] Mic.com. Available at: https://mic.com/articles/103600/how-politically-biased-is-each-industry-check-these-charts#.uPzAZ8klq [Accessed 3 Dec. 2018].

Sottek, T. (2018). *Burger King made a surprisingly good ad about net neutrality*. [online] The Verge. Available at: https://www.theverge.com/2018/1/24/16927890/burger-king-net-neutrality-ad [Accessed 9 Nov. 2018].

Stake, R. (2000). *Case Studies.* In: N. Denzin and Y. Lincoln, ed., Handbook of Qualitative Research, 2nd ed. Thousand Oaks: Sage Publications.

Stoltz, M. and McSherry, C. (2018). *EFF to FCC: Tossing Net Neutrality Protections Will Set ISPs Free to Throttle, Block, and Censor the Internet for Users*. [online] Electronic Frontier Foundation. Available at: https://www.eff.org/press/releases/eff-fcc-tossing-net-neutrality-protections-will-set-isps-free-throttle-block-and [Accessed 8 Nov. 2018].

Stone, J. (2013). Cyber War Will Take Place!. *Journal of Strategic Studies*, 36(1), pp.101-108.

Techopedia. (2018a). *What is Broadband? - Definition from Techopedia*. [online] Techopedia. Available at: https://www.techopedia.com/definition/794/broadband [Accessed 1 Jun. 2018].

Techopedia. (2018b). *What is Cybersecurity?* [online] Available at: https://www.techopedia.com/definition/24747/cybersecurity [Accessed 12 May 2018].

Techopedia. (2018c). *What is the Internet?* [online] Techopedia. Available at: https://www.techopedia.com/definition/2419/Internet [Accessed 1 Jun. 2018].

Techopedia. (2018d). *What is an Internet Service Provider (ISP)?* [online] Techopedia. Available at: https://www.techopedia.com/definition/2510/Internet-service-provider-isp [Accessed 1 Jun. 2018].

Techopedia. (2018e). *What Is Net Neutrality?* [online] Techopedia. Available at: https://www.techopedia.com/definition/2446/net-neutrality [Accessed 03 Mar. 2018]

Tews, S. (2017). *Repealing net neutrality: Implications for cybersecurity*. [online] AEI.org. Available at: http://www.aei.org/publication/repealing-net-neutrality-implications-cybersecurity/ [Accessed 9 Nov. 2018].

Turner, S. (2017). *It's Working: How the Internet Access and Online Video Markets Are Thriving in the Title II Era*. Washington, D.C.: Free Press.

U. S. Const. amend. XI, § 2.

World Bank. (2018). *Individuals using the Internet (% of population) | Data*. [online] Available at:

https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=US&name_desc=false [Accessed 8 Dec. 2018].

Appendix

Internet

As a standard definition for what is the Internet, Techopedia.com defines it as "…a globally connected network system that uses TCP/IP to transmit data via various types of media. The Internet is a network of global exchanges – including private, public, business, academic and government networks – connected by guided, wireless and fiber-optic technologies." (2018c). In essence, we are defining the Internet as the function of a system, rather than the technology and hardware that is utilized to make it function.

Broadband

Techopedia.com defines broadband as "…a high-data-rate connection to the Internet. The technology gets its name as a result of the wide band of frequencies that is available for information transmission. Information can be multiplexed and sent on numerous channels, allowing more information to be transmitted at a given time. The standard broadband technology in most areas is cable Internet, and asymmetric digital subscriber line (ADSL). The latest technologies are very-high-bitrate DSL and optical fiber connections." (Techopedia, 2018a). By this definition, we have a clear definition that broadband relates to the hardware and functionality of the network, rather than the content that is utilized on the network. Prior to broadband, Internet users utilized a dial-up service to connect to the Internet. According to the Center for Education and Research in Information Assurance and Security (CERIAS), states that the difference between broadband and dial-up is how a personal device connects to the Internet. A dial-up service "…connects to the Internet through your phone line. The modem in your PC 'calls' an Internet Service Provider (ISP) and connects with a maximum speed of 56,000 bytes per second, better known as a 56K speed connection. Each time your PC dials into the ISP, it is assigned an Internet Protocol (IP) address, which you can think of as an 'Internet address'." (CERIAS, 2018). CERIAS goes on to explain that broadband is different from dial-up in that a personal device is "…connected to the ISP through a cable or DSL connection, it remains connected until the cable box or DSL line is disconnected or physically unplugged. A DSL connection runs through unused wires in your existing phone line without disruption and can translate data at 5 million bytes per second, or 5Mbps. Broadband services are often referred to as "always on" services because it is not necessary to make a setup call to your ISP each time you wish

to access the Internet; this means that once you are assigned an IP address, you keep it until you request it to be changed." (Ibid).

Cyber Governance

According to the Working Group on Internet Governance in 2005 they defined cyber governance as the "…the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." (de Bossey, 2005, p. 4).

Cybersecurity

At the most basic level cybersecurity can be defined as the act of "…preventative methods used to protect information from being stolen, compromised or attacked. It requires an understanding of potential information threats, such as viruses and other malicious code. Cybersecurity strategies include identity management, risk management and incident management." (Techopedia, 2018b). The European Union Agency for Network and Information Security (ENISA) provides a more conceptualized space that cybersecurity works within. "Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace." (ENISA, 2016, p. 7). Furthermore, ENISA points out that the term 'information security' is a synonym of cybersecurity, as it means the "Protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system." (ENISA, 2016, p. 11). ENISA also points out that we should consider non-malicious disruptions as a threat as well, as human error can lead to serious ramifications. (ENISA, 2016, p. 10). Our primary definition of cybersecurity revolves around the action of providing security against threats. In practice, outside of a technological aspect, we must consider how then this translates to the field of international relations. According to Tim Maurer of Carnegie's Cyber Policy Initiative and Hannes Ebert of the German Institute of Global and Area Studies, "…the meaning of cybersecurity and information security has been highly contested. Broad definitions of the concept incorporate a wide range of cyberthreats and cyberrisks, including cyberwarfare, cyberconflict, cyberterrorism, cybercrime, and cyberespionage as well as cybercontent, while narrower conceptualizations

focus on the more technical aspects relating to network and computer security." (2017). Although the concepts within the subject of cybersecurity vary, Maurer and Ebert identify that they fit into specified areas in the field of international relations. "Scholars within the international relations (IR) discipline and its subfields of security studies and strategic studies increasingly focus on the technology's implications on national and international security. This includes studying its effect on related concepts such as power, sovereignty, global governance, and securitization." (Ibid).

Internet Service Provider

According to Techopedia, an Internet Service Provider (ISP) is "…a company that provides customers with Internet access. Data may be transmitted using several technologies, including dial-up, DSL, cable modem, wireless or dedicated high-speed interconnects…Other services, such as telephone and television services, may be provided as well. The services and service combinations may be unique to each ISP." (Techopedia, 2018d). Essentially ISPs are the intermediary force that provides the architecture and infrastructure utilized to connect individuals and organizations to the Internet. As the cables and hardware used for the Internet services are the same for telephone and television services, ISPs are able to bundle these services together based on customer needs. ISPs divide their customer base between individual and commercial needs. Commercial interest provide access for companies and organizations to the Internet, as well as providing digital business solutions. "In addition to providing access to the Internet, ISPs may also provide software packages (such as browsers), e-mail accounts, and a personal Web site or home page. ISPs can host Web sites for businesses and can also build the Web sites themselves." (Encyclopedia Britannica, 2018). ISPs are further differentiated between national and regional levels. Inc.com considers a national ISP as a company that provides "…Internet access in a broad geographical area. Compared to local ISPs, these companies tend to offer higher-speed connections and greater long-term stability." (Inc., 2018). Inc.com compares regional ISPs as small or independent companies that "…operate in many local or regional markets. These companies vary widely in size, stability, and quality of service." (Ibid). National level ISPs generally operate in regions that have a greater number of customers, whereas regional ISPs operate in smaller communities, filling the void in areas that national level ISPs don't operate.

Edge Provider

In 2014, prior to the *Title II Order*, the FCCs proposal for *Protecting and Promoting the Open Internet* defined an edge provider as "Any individual or entity that provides any content, application, or service over the Internet, and any individual or entity that provides a device used for accessing any content, application, or service over the Internet." (FCC, 2014, p. 67). To put this into practical use, an edge provider primarily refers to video and audio streaming services, electronic mailing and communication services, Internet search functionality, and digital database file sharing services. Essentially an edge provider offers end users the ability to utilize the Internet in a meaningful manner. However, the designation of an edge provider isn't limited to platform capabilities as the content that is utilized is not always created by these service providers. As Brett Frischmann points out "All end users provide content as they engage in communications with other end users, individually or collectively. YouTube content, for example, comes from end users uploading it." (Post, 2014). In essence we can then generally distinguish edge providers as vessels for storing or sharing content, and individuals or organizations that create content, both of which are not mutually exclusive of each other.

End User

The FCC defined an end user, within *Protecting and Promoting the Open Internet,* as "Any individual or entity that uses a broadband Internet access service." (FCC, 2014, p. 67). We can ascertain that from this definition an end user generally takes a passive role on the Internet as consumers of data and information, as well as individuals that utilize the services of ISPs and edge providers. However, Brett Frischmann points out that "…even passive 'consumers' communicate and exchange data." (Post, 2014). He goes on to say that as end users individuals may communicate with other individuals, share gathered knowledge through edge platforms, and so on. As he suggests it's hard to distinguish the line between edge providers and users, and that all end users are then edge providers. For this body of work, we should then define an end user as individual that utilizes the Internet as a means to connect to the Internet infrastructure.

Telecommunication Services

According to the *Code of Laws of the United States of America,* telecommunications is described as "…the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received." (47 U.S.C. § 153(50)). Additionally it describes that a

telecommunication service is an "…offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." Similarly, the Federal Telecommunications Standard Committee defines the action of telecommunications as "Any transmission, emission, or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems." (1996, T-4). Continued, the committee also describes that a telecommunications service is responsible for that transmission, whereby the customer of that service is responsible content of the message and the telecommunications service provider is responsible for "…the acceptance, transmission, and delivery of the message." (Federal Telecommunications Standard Committee, 1996, T-5). In all a telecommunication service is purely about the transmission of communicable information.

Information Services

According to the *Code of Laws of the United States of America,* information services means "…the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service." (47 U.S.C. § 153(24)). From this definition the FCC believes that ISPs offer the ability to be a vessel for user, which allows users to generate or retrieve information, utilize social sites, access news and media, and transforming and processing information online. (Federal Communications Commission, 2017, p. 9). Additionally, the FCC doesn't see ISPs offer a traditional telecommunication service in that user information may "…change in the form or content of the information as sent and received…" and that a user doesn't specify the process of transmission. (Federal Communications Commission, 2017, p. 10). Instead information is routed "…based on the architecture of the network, not on consumers' instructions, and consumers are often unaware of where online content is stored. Domain names must be translated into IP addresses (and there is no one-to-one correspondence between the two). Even IP addresses may not specify where information is transmitted to or from because caching servers store and serve popular information to reduce network loads. In short, broadband Internet users are paying for the access to information "with no knowledge of the physical location of the server where that information resides." (Ibid).

Bright-Line Rules

Bright Line Rules refers to "An objective rule that resolves a legal issue in a straightforward, predictable manner. A bright-line rule is easy to administer and produces certain, though, arguably, not always equitable results." (Cornell Law School, 2018). In the context of this work this rule refers to the three points adopted in the 2015 *Open Internet Order,* "1) No blocking - broadband providers may not block access to legal content, applications, services or non-harmful devices. 2) No throttling - broadband providers may not impair or degrade lawful Internet traffic on the basis of content, applications, services or non-harmful devices. 3) No paid prioritization - broadband providers may not favor some lawful Internet traffic over other lawful traffic in exchange for payment." (Rouse, 2018).

Light Touch Framework

The FCC moved to end Bright Line Rules within the 2018 *Restoring Internet Freedom,* replacing it with a light touch framework for regulation. This framework has three guiding principles: consumer protection, transparency, and reclassification. First, the FCC will be transitioning oversight of broadband to the FTC. Second, ISPs will be required to disclose their practices. Lastly, redefining broadband providers as an information service. (FCC, 2018a).

Bandwidth Throttling

Bandwidth throttling, also known as throttling, relates to the action of "Adjusting the amount of bandwidth to or from a server. The term is often associated with ISPs that limit the speed to users based on the volume or type of traffic being transmitted." (PC Mag, 2018). During peak times of Internet usage, ISPs practice throttling to help "…decrease congestion over their network, which lowers the amount of data they have to process at once." (Fisher, 2017). Congestion from processing data can then slow down speeds within the area network. Throttling occurs as an artificial cap to a customer's data allowance, throttling all types of traffic in an area, or controversially "…only when the traffic on the network is of a certain kind or from a certain website." ISPs may also choose to throttle bandwidth speeds due to the cost of outgoing transmission of data to users, where "…average monthly wholesale prices for bandwidth vary from $30,000 per Gbps/month in Europe and North America to $90,000 in certain parts of Asia and Latin America." (Marcon et al., 2011).

Blocking

The FCC considers blocking as the "…failure of a broadband Internet access service to provide an edge provider with a minimum level of access that is sufficiently robust, fast, and dynamic for effective use by end users and edge providers." (FCC, 2014, p. 67).

Paid Prioritization

According to the *Code of Federal Regulations* the term paid prioritization, or data discrimination, refers to "…the management of a broadband provider's network to directly or indirectly favor some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, resource reservation, or other forms of preferential traffic management, either; (1) In exchange for consideration (monetary or otherwise) from a third party, or (2) To benefit an affiliated entity." (47 C.F.R. § 8.9(b)). In practice an ISP would implement a "fast lane" for edge providers to ensure their data stream is uninterrupted. Large edge providers claim that "…fast lanes would make Internet service providers (ISPs) gatekeepers and give them the power to influence free market activities. Smaller edge providers fear that once an established site has been prioritized, it will dominate competition and stifle innovation." (Rouse, 2018).

Norges miljø- og biovitenskapelige universitet
Noregs miljø- og biovitskapelege universitet
Norwegian University of Life Sciences

Postboks 5003
NO-1432 Ås
Norway