A Fight for Your Information; or How I Learned to Start Worrying and Fight out Censorship

Researched By: Christopher Stevenson
Overseen By: Professor Pamela Warren

Since the dawn of civilization, people have requested the right to be heard, to be listened to - and with that power, have the right to share information and things deemed useful and important for others to see and hear. In the most present era of communication, the platform to be best heard on has had many iterations; but ultimately the most major medium which has altered history is the internet. While the internet has been an immeasurably useful tool for advancing global communications, unfortunately, there has been a widespread belief that a modern form of persecution of speech could be avoided, and the free flow of ideas on the internet would remain unaltered; history has decidedly chosen otherwise. Censorship is a word most people are familiar with, having been a concept in some shape or form present in most major civilizations since the dawn of humanity itself - which would ultimately include the present era as well. Considering that, there are a few questions we, the current general public, should ask ourselves as intrepid pioneers of the digital era: How is our digital information and media controlled and censored in the modern era? What are the consequences of these actions or inactions? There are many different answers and views which can be disseminated on this topic. My personal perspective, which I will show in full researched detail, within this paper, is that the internet has become a, if not the, primary source of information channeling in the modern era (for a multitude of different reasons) and while this has opened up channels of communication globally, it has not been without fair appropriation of censorship - at this point, no country truly has a free distribution of information and content, which is okay as it therefore advocates for a modern, decentralized model of existence for people worldwide. The former standard where people rely on the legal and metaphorical internet freedoms of one nation alone, may fall to the wayside in favor of what I have coined a “decentralized individual communications model”; which is opposed to the former ideal of singularly “having all your eggs in one basket” when it comes to having a presence to post and see things on the internet.

The history of how people came to choose to interact and share information and content on the internet, has a very understandably long and intricate timeline of inventions and services which have either slowly progressed over time or have been rapidly discarded in favor of more authentic and modern methods of communication.While the technology that built the first computers has been around for decades, the digital communication connections which have upheld and advanced the internet are relatively recent developments; the world wide web, and the subsequent further development of the concept of the internet, has only been around since the early 1990s, created by renowned computer scientist Tim Berners Lee.(Burgess 2017) Seeing as the easiest methods of communicating at the time, in the 1990s, was through the telephone, ultimately the first reliable method for setting up the further infrastructure that became “the internet” was through telephone pole connections across the world. While satellite providers came into greater existence for cell phone providers later on, ultimately telephone companies and individual internet servicing companies became collectively known as Internet Service Providers - otherwise more commonly known in shorthand as “ISPs”. While ISPs could in turn provide access for individuals to “be online”, they do not provide the actual content that is found on the world wide web or the general internet; other people upload or share whatever content they deem fit to be hosted on the internet, through website hosting and server hosting, or by posting on websites which have been hosted by others, under the guidelines of those websites rules. These individuals (and companies) who primarily host are known as Web Service Providers - or more commonly known in shorthand as “WSPs”.(Heckmann 2006) Together, these two different providers help makeup and uphold the majority of hosting for all digital content and information that can be and will be seen on the internet; that would include every post on common and popular social media websites we read everyday, articles by news congregating outlets we view occasionally, and the ramblings of weird kooky websites we visit when we want to put our own crazy thoughts out into the world - all of these websites are forms of digital information, which are stored and hosted on the internet by these providers.

(Heckmann 2006 and Burgess 2017) In answering questions of how our digital information and media is controlled and censored in the modern era, this leads to the natural question of how ISPs and WSPs interact within their respective industries; how is it feasibly possible for ISPs and WSPs to be competitive with other companies? How do these companies within the communications industry run their operations in the first place, without breaking overwhelming rules? What legal protections are in place for consumers and for operating companies? These are important questions to ask and answer, as arguably most of our modern approaches to sharing content and information with each other relies on using the internet or some other similar digital format, whether it be a website, or an app, or a social media platform - therefore it would be useful to know how these digital providers choose to operate, and in some cases must operate under the law.(Heckmann 2006 and Burgess 2017)

The first question I proposed which should be approached is how ISPs and WSPs are allowed to be competitive in their respective industries - this is the first question to approach because the field of discussion in this area is relatively narrow, as ISPs and WSPs are often subject to serious scrutiny and oversight in their own productions and maintenance.A poignant reason ISPs and WSPs are subject to serious oversight, is the fact that both industries collectively have seen a massively dramatic rise in daily users and therefore competition, as the necessity of using the internet grows with each passing day. Ultimately, to separate themselves in a sea of competition, both forms of providers must “run efficient businesses with a specific trait which sets them apart from other companies” - sometimes this is in the form of a “ultra secure network”, sometimes the network architecture might support a greater capability to share content and information faster; commonly what's seen offered is a model centered around “adequate amounts of quality of service”; whether that be in the form of customer satisfaction or offering incentives to users, the definition of “quality” varies wildly. At the same time, ISPs and WSPs must consider the future of their industries as well; as fast as the internet grows in popularity, users will not remain stagnant on the same websites, using the same features for

digital sharing forever - tastes, and people, change over time. Therefore, it also becomes important for providers (particularly ISPs) to invest in emerging technologies like “Voice over IP (otherwise known as VoIP), peer-to-peer sharing, and network gaming.” Currently, these providers are given some leeway in being able to entice users to use their communicative platforms, yet in the scope of “competitive economic markets” there remains to be a serious effort created in recent years (within the North American market at least) due to restrictions on how media providers are allowed to present themselves. (Heckmann 2006)

The second important question to address regarding ISPs and WSPs is how these providers are able to run their respective companies in each industry, when there is a great deal of governmental (and citizen) control and oversight, enforcing easily breakable rules. This question is particularly important to review, as there is a large amount of prior established legal procedure behind the history of the internet and its advancement to its current iteration. For decades, most local and international judicial systems were woefully behind on understanding the internet and how to issue just rulings on issues occuring within the sphere of the digital world. Individuals who use the internet, are expected to not break the general laws of their home country on the internet, but otherwise are often given a pretty free experience to roam and share online. Providers who serve individuals on the other hand, must be very aware of a largely different set of rules, for conducting activity on the internet; most of the time providers are expected, at least in some part, to lightly monitor the content that is hosted on their servers or through their hosting capabilities. Notably, WSPs must take into account these rules with much more seriousness, as they are the companies responsible for running servers of information (websites, etc), capable of distributing said information to others on the internet. In some regards, and in some legal considerations, these web providers are also holders and possessors of whatever information is held on their servers. Therefore it is of the utmost importance for WSPs to not be hosting violent or threatening content, which would be a violation of the first amendment.(Dinwoodie 2017) Looking at it another way, WSPs should consider the

internet a general public meeting platform - except these domain masters and other moderators must consistently clean what is said or shared on the platform themselves, as to avoid being liable for what might be done that is (possibly) illegal. The term for this is known by some researchers and authors like Dinwoodie, as avoiding becoming a “secondary liability”.(Dinwoodie 2017) Commonly this phrase is used to define the different manners in which a WSP or an ISP might be held liable for some ways in which third parties may engage in unlawful activity - which could involve infringements upon “copyright law, trademark law, and defamation law” - and these claims are on the rise, with some countries even opting to delineate the exact means of “true secondary liability” with intermediaries in some contexts.(Dinwoodie 2017) The takeaway from these revelations is that at least in some aspects, our current primary source of information in the modern era, may be threatened by the legal ramifications of an internet or web provider becoming challenged by these “secondary liabilities”. If someone were to issue a legal claim to a provider, about some form of information or content on a website or app that they were unhappy about, the website and information itself could be “shut down” and removed due to secondary liability, therefore threatening the free flow of information on the internet.

The final major question to ask about the nature of ISPs and WSPs is if there are, if any, legal protections in place to prevent liabilities and risks for entities involved in internet services. This question seeks to answer whether or not providing companies and consumers of these services are legally protected from liabilities in any limited manner themselves. The answer to this question is long, but necessary for understanding exactly what legislation is regarded as the “most important” or currently relevant towards navigating the internet; most times these issues are treated in the public as major points of contention, worthy of either making or breaking the sanctity of the internet. One major concept which once was in place was Net Neutrality. Net Neutrality, in short, is the concept that legally, the internet has become a near daily necessity and utility for most people; and with that consideration, there are legal permissibilities and

restrictions which should be put in place.(Belli 2015) Another concept which has been debated endlessly is the imperceptibility of copyright law, and why the system of legal justice for copyright holders and users alike is woefully and irretrievably broken in the current state that it is in - meaning that important pieces of information and culturally significant pieces of content are being ill-fittingly censored for being shared online freely. This unfortunate process has been a concept developing for decades now in different mediums, and has only gotten progressively worse, while only illuminating small blips of hopeful change in others. The most highly discussed legal issue of late 2020, defining much of the current discussion behind the infrastructure of the internet is related to the repealment or amendment of the 1996 Communications Decency Act; more specifically, subsection 230, which provides and I quote “immunity from civil liabilities for information service providers that remove or restrict content from their services they deem "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected", as long as they act "in good faith" in this action.” (Ruanne 2018) In easier terms, section 230 protects internet website owners and hosting providers (or otherwise known as Web Service Providers) from serious criminal or civil liability if one of their users or visitors happens to post content which is severely questionable or unsavoury to others. This can include a variety of different forms of content. Once again, it is important to review these legal concepts with nuance, as they pertain to most of the discussions surrounding the sharing of information and content in the modern era, through the internet. The difference between having these legal protections remain in place or become fully repealed, ultimately changes the entire legal framework of the internet in the United States, as well as inevitably in other countries as well. Our collective ability to distribute and see information and content freely on the internet, and to avoid censorship, likely lies in the final legal verdict of one of these three legal predicaments.

The oldest and most ruthlessly debated of these three legal affairs is the issue of Net Neutrality. Network Neutrality mandates to treat internet traffic in a non-discriminatory fashion in

order to maximise end users' freedom and to safeguard an open Internet. At one point, the practice of Net Neutrality had the legal ramifications to allow the internet to be considered a “necessary utility” of everyday life, and that ISPs would have to treat internet traffic in a non-discriminatory fashion in order to maximise end users' freedom for an open experience on the internet - meaning that it would be much harder for ISPs to simply remove you from their rooster of services without much warning or reason.(Belli 2015) While no longer a legal requisite in the country due to recent changes, at one time according to the United States government since the internet has seemingly become a daily utility for most people, then it should be legally accessible to all, like other daily necessary utilities, such as having running water, flowing electricity, piping gas, and many other similar services someone might face a utility bill for. The internet should not be prohibited from use for some due to a company's personal beliefs, whatever they may be, and therefore as long as someone can pay for the service, they should receive it. Along with this belief, Net Netraulity used to encompass that legally companies should not be able to “throttle” your internet or punish users, because you are a low paying customer; in other words, users should have set abilities to purchase data, with no discrimination of service to any one user or group of users in particular. (Belli 2015) In many cases, by those who champion Net Neutrality laws, these protections are viewed as nearly part and parcel to being human rights; as necessary daily utilities should be available, and consistent for those who need them to live their daily lives. They see the removal of these protections as the grant to allow for companies to discriminate, throttle, and squander services to those who are either low paying customers or are otherwise undesirable in one way or another. Alternatively, those who are against net neutrality rules have a far different perspective on the issue of Net Neutrality guidelines; they believe that the guidelines unfairly stifle competition specifically within the internet service provider industry. They believe that due to these archaic rules being put into place, internet providers are left stuck supporting the same outdated systems of digital communication, as their ability to upgrade their equipment, physical lines, or

general services is severely inhibited by possible action by the Federal Communications Committee, more commonly known as the FCC, which oversees and issues fines related to problems of this nature. (Belli 2015) Internet Service Providers themselves have maintained the perspective that other countries and localities have had the ability to upgrade their services for years, resulting in other nations and continents having vastly faster internet service than the United States. While the public and popular discourse behind Net Neutrality began in 2011, almost exactly a decade ago, the ultimate conclusion of these discussions was an FCC ruling in 2017 declaring the principle to be dead, null, and abolished in practice, therefore at least for the moment ending Net Neutrality as a feasible ongoing concept to continue in the United States. Since 2017, there have been various reports from various sources claiming “internet speeds overall are up” and alternatively “throttling in certain regions has gotten worse" There has also been discussion with the newest presidential administration under Joe Biden, to encourage the FCC to reinstate the principles of Net Neutrality; however nothing has taken place on that front, at least as of yet. While other countries have some variations of laws similar to Net Neutrality as it once was in the United States, as it currently stands, the practice is fading into historical obscurity until further notice. However, if the debate behind Net Neutrality were to resume in the recent future, there are three important aspects of continuing discussion that must be overcome, in order to have a solid and stable Net Neutrality legislation accepted by many in the future going forward. These obstacles to conversation would be to “avoid polarization on the issues, clinging to historical remnants and perspectives of the internet, and to consider up-to-date competition analysis.”(Belli 2015, pp. 213 - 225) In addressing discussions of Net Neutrality in this manner, most perspectives of Net Neutrality are considered, and worked through in a thoughtful and united way. While the current removal of Net Neutrality laws in the United States appears to show that major companies seemingly have the right to “quash” you out if they so desire, that has so far been unlikely but debatable as to whether or not the situation ever got worse because of the repeal of Net Neutrality. Of course, only due time can truly tell of the

ramifications behind removing Net Neutrality; however there are a series of other protections and issues which are currently far more important to the collective - and your individual - future on the internet.

The most highly discussed legal issue of late 2020, defining much of the current discussion behind the infrastructure of the internet is, perhaps surprisingly, the Communications Decency Act of 1996 - and more specifically subsection 230 of the act. As described before and above, the act containing section 230 was passed in 1996 to combat a growing internet user base, ill-informed of the legal ramifications and specific liabilities of certain actions on the internet. In 26 short words, it defines that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."(Kosseff 2019) In other paraphrasing, it “defines that an information service provider shall not be treated as a "publisher or speaker" of information from another provider.” and it “provides immunity from civil liabilities for information service providers that remove or restrict content from their services they deem "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected", as long as they act "in good faith" in this action.” (Ruanne 2018) While the Communications Decency Act of 1996, and section 230 may appear to be a roundabout good nature policy, set forth to protect creators and providers on the internet from extreme liability in posting online, there has been a recent fiery debate set forth within the past year; arguing for the amendment of the original act to allow for greater liabilities towards those who publish unsavory information about others. While it appears as though this issue was raised during the last presidential administration, it appears as though the thought of this effort has bi-partisan support, and historically efforts to limit the scope of immunity have succeed on a federal level, with rulings against Roommates.com and Accusearch in 2009 having been successfully upheld. (Kosseff 2019) So what is attributing to the erosion of what seems to be a basic right of passage on the internet? Section 230 does not limit liability completely, and it never has; it merely

suggests that providers and in some instances, creators and users, should be provided the opportunity for limited liability, in cases where good faith is adjudicated. Some institutions have claimed that this erosion has come from both very real and imagined issues stemming from section 230, and have examined the very real possibility that section 230 of the Communications Decency Act could be amended or completely revoked within the coming months. What would that look like on a national scale? Or even an international scale, considering a rippling effect within the legal structure of the internet could become a very real possibility. Supporters of section 230 remaining the same contend that any changes to the law could come with devastating consequences for competition, innovation, and free speech - which would translate to legal chaos as well. The ITIF, or the Information Technology & Innovation Foundation, have public debates on the topic and have released a comprehensive report on a three step plan to uphold section 230 provisions for everyone's benefit. The ITIF suggests, that in order for section 230 reform to work, there would need to be an establishment of a good faith requirement to the first portion of section 230 which states “an information service provider shall not be treated as a "publisher or speaker" of information from another provider”, a prevention measure against nuisance lawsuits working with the same good faith measures, and third expanding federal criminal laws to be included within section 230’s existing exceptions for federal law (Feeney, Perault, Johnson 2021). In essence, the ITIF argues that these measures would curtail all of the current issues, real or imagined, which have arisen from the implementation of section 230 in 1996. While I believe this could be true, there is a larger picture at frame which the ITIF did not (at least immediately) address - the fact that the international legal structure in place for the internet teeters closely off of changes within other countries' judicial systems - especially the United States. Therefore, any changes of section 230 within the United States, regardless of possible valid features of reprieve, will have consequences and implications on an international level, which in turn could either threaten or aid freedom of sharing information online. Whatever the next few months, years, or decades

may hold for section 230, the main takeaway for citizens should be that section 230 is currently allowing for websites to continue to post information and content which may be deemed “unsavory”, unlikable or possibly even untrue to others, without extreme liability for doing so - revoking or altering that protection too heavily will cause a disturbance in people's abilities to share things freely without fear of retribution on the internet, and will therefore cause a voluntary censorship among those who wish to not be liable for large fines in heinous damages. As it currently stands, regardless of whether you are a supporter or not, section 230 of the Communications Decency Act protects the free flow of information and content on the internet, and the rights of others to contribute to the flow - for better or for worse. Any alterations or instability in section 230 will severely put into question the concept of censorship, whether it is formally voluntary or not.

The last major legal digital - and non digital - based issue which is discussed in the fight for freedom of information and content sharing, is the currently inadequate and inept copyright claim system, which has a basis in US law and international law alike. One of the most common ways people tend to find themselves dealing with internet copyright claims, is through violations of the Digital Millennium Copyright Act of (1998) - also more well known as being served a “DMCA Claim”. A DMCA claim essentially demands whoever is hosting content that is potentially copyrighted, to remove the content immediately - or in some instances, there can be agreements made where if the content received income, it would go directly to the copyright holder as a form of royalties. Many creators on YouTube and other platforms developed for sharing ideas and content, have faced these claims head-on, with some individuals famously taking their cases to court. Ultimately while the DMCA of 1998 protects copyright holders' protections, there are cases in the United States where under section 512 providers can be granted a form of “safe harbor” from legal liability in DMCA claims. There are at least three types of defined safe harbors within copyright law, the first being a safe harbor from “conduit”, the second being a safe harbor from “storage caching”, and the third being a safe harbor for “hosts”

- or as have defined more broadly “providers”.(Wang 2018) In essence, within the United States, these three protective guards shield from potential copyright liabilities stemming towards web service providers, website providers, web storage providers, and web hosting providers - all industries of which I have defined as Web Service Providers (WSPs). In many cases, content creators and sharers can go by the “tried and true” method of copyright liability prevention; mainly that would mean whatever copyright content is being discussed, must be altered or commented and critiqued on - in the eyes of the law, by doing this, content creators are intrinsically changing the original nature of the copyrighted content, and the shared information or newly cultivated content becomes a new format of medium on its own. There have been at least two major cases where these miniscule differences have been settled, and clarified for everyone in a courtroom. A case stemming from 2016 originating on YouTube, where two popular commentators - Ethan and Hila Klein - were accused of stealing copyrighted material from another platform commentator, and were subsequently sued due to a irreconcilable difference of opinion on the issue. The defendants, the Kleins, argued that the work they created featuring the plaintiffs original clips constituted fair use, as the new content created by the Kleins was “transformative and commentative” in nature. After a trial period, the Kleins went on to win their case, with the presiding judge saying “there is no doubt that the Klein(s) video constitutes critical commentary (and) is decidedly not a market substitute for the (copyrighted videos in question)” in favor of their win. (Hosseinzadeh v. Klein 2016) On the other hand, copyright law has also been established through past cases (perhaps egregiously) in favor of copyright holders. Napster Inc. was an early 2000s music sharing and downloading platform, which gained nearly overnight fandom and popularity for offering a website dedicated to sharing music and mixtapes with others around the world. The music that was often offered on Napster was from major musicians and artists from around the world - without any prior express written permission to do so. This lead to a major legal case which established Napster as a vastly divisive entity of the early internet era - some people loved their services, while others clearly

did not. Napster had been in existence and wildly popular for about one year before it was finally remanded to be shutdown by court order of the federal government, stemming from an earlier civil suit; Napster had lost their case.(A&M Records, Inc. v. Napster, Inc. 2000) Of course, these two court cases are not the first, nor will they be the last, to change the landscape of copyright law in the United States - which is not considering the vastly different legal landscape behind copyright law in other countries and regions such as China or Europe. The truth is that the copyright system as a whole is vastly broken, which must be fixed on all levels digital or otherwise in order to become saliently useful for stopping egregious copyright violations. In the meantime, because of the flaws of the current copyright claims system, users of the internet should be wary that the information and the content they post could be subject to a random copyright claims and DMCA takedowns, either initiated on occasion by ill-informed individuals or malfunctioning algorithmic bots.(Scott 2020) While in effect this could potentially be easy to negate away, or to shirk off because the system as a whole is broken, users of the internet could be and are occasionally subject to undue legal burdens, which curtail the free flow of information and content online. In effect, this acts as another form of voluntary censorship.

These discussions revolving around the most important and relevant legal affairs surrounding the free flow of information and content on the internet, leads to even further questions which must be answered, if we are going to truly answer the question of how our digital information and media is controlled and censored in the modern era and what the consequences are for actions or inactions taken by users disseminating information on the internet. As novice observers, we can be aware of the legal protections and ramifications which citizens and companies in the United States must uphold; but these verdicts do not often translate into real life scenarios which work legally perfectly well. On the other hand, certain rules to the internet that must be followed through US communications technology and by US individuals and companies, may be legally more acceptable in other portions of the world. Slowly as time goes on, we are seeing more and more examples of this being true in practice;

other countries may opt to engage in practices, which could give them an economic, political, or other advantages. Internet Service Providers, Web Service Providers, the government, along with a multitude of other surprising entities and figures can control and manipulate certain internet protocols in a variety of different ways, for a variety of different reasons. These entities to some degree are known as the “gatekeepers to the internet and cyberspace” since, often these entities are responsible for monitoring and regulating a portion of communication on the internet.(Laidlaw 2015) I think it is important to review cases where communication was monitored and consequential on the internet, as these events can be heinous, but they can and have also established many legal rights, and questions about our civil liberties, after verdicts have been reached appropriately. While many cases of digital communication monitoring have been internationally based, or have been “un-chargeable” in a court of law, they still remain significant to review as these cases have had effects on people and places around the world. These cases and instances have ultimately shaped our modern infrastructure of the internet - therefore these gatekeepers to the internet have helped shape the flow of sharing information and content on the internet, and continue to do so to this day.

Some countries, by their respective governments, are choosing to slightly manipulate the means of internet communications for their citizens, in order to achieve certain gains such as political censorship or greater economic benefits for the country or for a specific region itself. Some countries are well known for this practice, and have benefited from its usage: the largest country that often comes to mind is China. Take for example, the recent economic swelling of Chinese national corporation, Alibaba; Formed by Jack Ma in Hangzhou in 1999, Alibaba is well known in China for being the premier general internet marketplace, as Amazon is known in the western hemisphere the same way. This popularity is not a coincidence, as many favorable outcomes worked in Alibaba's favor - Amazon did not enter the Chinese market at all until 2004, and eBay did not enter until 2002, which gave Jack Ma a considerable advantage marketing his company to a market of one and half billion immediately nearby citizens. Even more favorably,

with the help of the Chinese government, media, and Alibaba's marketing team, retail holidays have been set up strictly to act as vehicles for explosively funding the economy; this would be in the form of "Singles Day" or November 11th. A relatively recently established "holiday" it serves as an ode to bachelors and bachelorettes who are still single - tempting them to purchase lavish gifts for themselves for a discount price. This concept is very similar in nature to "Black Friday" within the United States - however, I would argue that Black Friday is less propagated by the ruling government, and mainly just serves as an excuse for businesses to clear storage of old products while making profitable gains in the fourth quarter for business reports. Regardless, Singles Day, as contrived as it may be, has been a massive success in China, pooling in a record $74.1 billion dollars in gross sales in 2020, ultimately helping keep Alibaba and China's economy monetarily strong.(MIT Tech Review 2016) This also occurs in alternative online industries, such as with social media; for many years Facebook (has/was/is) been banned from users in China, for a variety of different reasons. However the alternative social media platform which arose from Facebook (and other websites) banning was Chinese national corporation Weibo - which has now gone on to become popular in markets outside of China. (Issitt 2019) The takeaway from this, is that ultimately while the idea of progressive globalization of the internet and our communications may flourish in some ways, it falters in others; this is particularly true when discussing the internet and the free flow of information and content - at least in certain countries and regions, the flow of communication offering alternate products, services and information itself, is reneged to allow for a nationalistic advantage. This concept of controlling the means of communications for some form of gain, is very likely present within this story of Alibaba and Weibo; yet it applies to multiple industries and countries worldwide. We must consider collectively, if these actions are a dereliction of internet users abilities to freely and easily access any and all information and content - even that which is "unsavory", unlikable or acting in "bad faith". Are internet users who are citizens of particular countries in some ways, being prevented from accessing all forms of information and content, and are therefore being

censored from the full scope of the internet? In many ways, through simple observation we can argue that manipulating the internet in this fashion places an undue burden of silence and possibly even censorship on users and companies operating in these industries.

As bad as potentially manipulating the internet to encourage citizens to purchase local and national products alone may be, there are some countries and entire regions of the world which openly shun and criminalize particular behaviors related to sharing information and content freely on the internet. Generally speaking, many countries with authoritarian governments are often subject to this harsh treatment, with citizen journalists, activists, and bystanders alike being corralled into criminally lengthy legal sentences for having shared an opinion, or for being too digitally “present” at the wrong moment in time. This treatment, while much worse in some parts of the world, is indiscriminately present in most countries and places, as is the case with a variety of different situations arising separately out of China and the United States. For instance, in 2010 Chinese courts chose to jail a Uighur Journalist for 15 years, for reporting on matters related to the ongoing Uighur-China controversy by speaking to foreign journalists; the controversy which claims that the minority Uighur people of China are being placed in re-education concentration camps. Gheyret Niyaz, owner and operator of the website Uighurbiz.net, was given an unusually harsh sentence, as admitted by the Chinese government, in an attempt to fight “threats from radical groups fighting for Xinjiang independence.” Even overseas Uighurs were surprised by this move, as Niyaz was broadly supportive of Chinese government policy. (Graham-Harrison 2010) This practice has also been common in other major countries like the United States as well; a prime example of this would be Sammy Rivera of Philadelphia. In 2020, amidst the series of various protests which broke out for a variety of reasons in the summer, Sammy Rivera decided to take photographs of what he saw to put them online to share with the world. After a few posts on Instagram, he began to feel weary about possibly sharing the identities of individuals who could be identified easily with everyone online - so with one final post on the subject, Sammy decided to stop posting photos of people he saw

at the protests. Less than one week later, Sammy was arrested with five other people, for allegedly vandalizing a state police vehicle. According to the FBI, when they saw photos of others around vehicles set on fire, they set out to arrest those individuals - with Rivera being seen taking photos of the incident with his own camera. (Shepard 2020) While Sammy Rivera has not been prosecuted yet, these incidents should underline to internet users that the freedom to fully share information and possible content which might be taboo or unsavory or unlikable is always at risk; as citizens of certain countries can be manipulated and encouraged to look at certain content, people can be banned and discouraged from sharing and reviewing content which is deemed unfit for public consumption. Both of these behaviors severely limit the capabilities of a free exchange of information on the internet.

While in some countries, governments have been the main contenders for controlling the flow of information and content, there have been some unique situations where it seems private digital companies, organizations, and institutions with a basis on the internet will block and prevent particular individuals from many major facets and utilities of society and daily life. This concept has become known as being “cancelled” - a referral to the fact that (at least purportedly) the individual or group in question being “cancelled” is or will be completely unable to function using most major services online, and should be promptly discarded from public thought. While this concept has been debated thoroughly in recent years, researchers Paul Barrett and J. Grant Sims at NYU Stern decided to look into the issue surrounding cancellation on social media, to see if what was being purportedly said had any merit - that individuals on average are being canceled more often, and more specifically conservative voices in the United States at the moment are being censored and banned from using most major and sub-major platforms. After extensive research, Barrett and Sims reached the conclusion that while there could be an argument in favor of general censorship uptick, the claims that conservatives are being censored on average more often on social media is unfounded and relatively baseless. They claim that “the notion of anti-conservative animus itself is a form of disinformation: a

falsehood with no reliable evidence to support it.” They argue that even upon closer examination, these claims of bias tend to crumble easily - when the platforms being argued as censors gave a considerably wide berth to conservative voices, noting that conservatives and dissidents on social media are often the most followed pages, with the most engaging content on these various platforms - whether it be Facebook, Twitter, or some other form of social media. On other occasions, social media platforms went out of their way to appease claims of censorship on behalf of conservative voices; in one instance in 2016, it was reported in a Gizmodo article that two anonymous Facebook employees claimed a once popular feature called the “trending topics tab”, routinely removed articles and information originating from right-wing sources. In response to this article being released, Mark Zuckerberg invited the largest conservative commentators like Glenn Beck and Tucker Carlson to his Facebook Office in Menlo Park - a short amount of time later, he proceeded to fire the trending topics tab staff, and shut the feature down completely.(Barrett & Sims 2021) In four steps, Barrett and Sims argue censorship can be removed from social media and people can begin to trust these platforms again; by providing greater moderation disclosure, separate moderation algorithms to choose from, human moderation of larger accounts (as opposed to bot moderation), and last but not least to release more data for researchers to review - which also solves problems of disclosure and privacy. (Barrett & Sims 2021) No matter how you feel about the findings of Barrett and Sims at NYU Stern, their research and preliminary questions did not go in depth enough to examine another new concept within this same realm of activity and thought; being “deplatformed” - or to otherwise to be “cancelled” and censored so hard, that individuals may not have access to basic daily utilities, such as having a bank account, or an insurance policy. One of the most well known individuals to face this consequence was Alex Jones. As explained by the New York Times, Alex Jones was officially banned from banking with PayPal, in both a business and personal manner. Along with this, Alex Jones InfoWars app was removed from both the Google Play and Apple store, and has since not returned. (Popper 2018) Another

similar instance of potential deplatforming which recently took place, was an apparent cancellation of famous former pitcher Curt Schillings AIG insurance policy, which according to AIG was reportedly due to “hateful and insensitive” comments made by Shillings on social media. (Golding 2021) Due to predicaments like Alex Jones, InfoWars, Curt Shilling and others (whether you perceive these consequences to be for better or for worse) along with the growing both real and imagined belief that “cancel culture” and censorship exists, there has been a growing distrust from those who believe they may be persecuted on the internet. These individuals and groups do not believe as though they have the full capabilities to post and share information or content which they perceive as interesting or unique - therefore many people of these groups have begun to create what is becoming know in some circles as “the Splinternet” John Gilmore, famous internet pioneer of the 1990s, often said “the internet interprets censorship as damage, and routes around it.” which is exactly the case of what happened with the creation of social media sites like Parler and Gab.(Lemley 2021) As mentioned briefly by Barrett and Sims, due to this distrust of social media some individuals have flocked to using new social media apps like Parler, a right leaning twitter-like alternative social media app, and Gab, a consortium of alternative based social media and sharing services.(Barrett & Sims 2021) In recent months, since the event at the Capitol on January 6th 2021, these “splinter-sites” were removed from the Apple and Google Play store respectively, threatening the abilities of users to download, update or view anything within the app. After a series of lawsuits and arbitration, Parler has since been readmitted to the Apple store, after meeting the guidelines previously accused of being broken, while Gab continues to contend the issue in court. While the concept of people having access to more social media outlets outside of the major few is good in nature - it encourages competition within the industry, as well a decentralized model of communication where internet users can share with much greater freedom and expanse - it can in effect launch platforms which insulate people to new or other ideas. This is why in an ideal situation, as mentioned by other researchers, major social media outlets remain open, honest, and neutral

regarding most issues that aren't explicitly illegal, so that internet users can be exposed to a variety of different beliefs, information, and content which is relatively unbiased and recently pertinent as opposed to being insulated with one narrow perspective of belief and set of concerns. The honesty of social media and other major sharing websites is crucial towards upholding a trusted and open internet for everyone, where the flow of information and content flows freely.

When speaking on the belief or conviction of censorship on the internet in the form of "cancellation" in North American, people should be aware that this debate is taking place on full display on the world stage, and it has ultimately been underpinning faith in western digital freedom. Major dissidents of the United States have made remarkably bold statements reprimanding and underlining very public instances of censorship, and the concept of its existence in silicon valley. Russian governmental agents as well Russian President Putin himself have claimed that in the United States there has been a rise of "IT exceptionalism" - essentially declaring that only those who think and act exceptionally, have the right to use the internet fully. This exceptionalism, Putin argues, is creating what people are seeing as the "big tech ideological divide" - which is creating a "serious challenge" by restricting users access to sharing and receiving information and content which may be deemed important or necessary. (TASS Russian News Agency 2021)Comments like these are not uncommon by the Russian government, or other dissident governments for that matter - yet they illuminate two very real problems for the United States and western digital communications. The first problem is these comments underpin the actual true freedoms United States citizens have while using the internet, which in turn creates a greater sense of uncertainty for those who already possibly believed the internet was censored or is beginning to become so. The second issue is that due to these comments, and the growing weariness of trust in internet freedom within the United States, people may find that other countries are possibly offering better options for hosting certain forms of speech, information, and content. In turn, this creates what I have defined as a

“decentralized individual communications” model; where as opposed to relying on one predefined system and therefore “putting all your eggs in one basket”, internet users opt to diversify their content to be hosted and provided everywhere. An example of this might be where someone who wants to host a taboo website, chooses to register their domain name in Russia, while hosting their content online in Germany, or the United States, discussing affairs in China or anywhere else for that matter. In that way, internet users are protected from a barrage of censorship or any untimely events which may remove their content from visibility online. Ultimately comments like these from Russian government officials underpins faith in freedom from censorship in the United States - these types of remarks serve as reminders to erode the faith (of those who listen) in the ability of the United States to provide a free internet experience - surprisingly in some cases, perhaps maybe even the Russian government is correct in their statements that certain freedoms that are set forth in Russian internet are not ascertained here. In either regard these comments serve as fodder towards denigrating the faith of those who already were losing faith in the ability to share information and content freely on the internet - therefore these comments create deeper and more serious divides in unity behind general public consensus of freedom on the internet.

After everything that I have noted, among other unmentioned more heinous cases, there may exist some skepticism about the full freedom of individuals rights to use the internet. More specifically, there may exist skepticism whether users of the internet in the United States (or anywhere else really) should worry about the possible dangers which might arise from questionable internet use. Fear not however, as history has seemingly shown that if you were to find yourself in the midst of a lawsuit or even a possible criminal complaint, it is very possible to find legal justice through the endless legal appeals system, or through talented, well-informed lawyers. Unlike most other legal systems present within other countries, the United States has an extraordinarily complex, forgiving, and long winded legal appeals system, which has helped find justice for many people in the past - with internet users being no exception. There have

been many cases around the world, but particularly based in the United States, which gained traction as having been significant for gaining rights for internet users to post information and content deemed fit for public consumption. One of the most prominent cases in recent history defending the right to post content which is protected under copyright law is the case I mentioned previously with the Kleins, two famous YouTube commentators. Their lawsuit specifically had noted from the judge that their content was “decidedly not a market substitute” and therefore was “fully constituting fair use (practices)” (Hosseinzadeh v. Klein 2016) One of the most prominent lawyers in the field of internet defense work is Eben Moglen. A professor at Columbia University School of Law, Moglen has defended a series of important pioneering internet legal briefs, ultimately helping keep several important pieces of technology that make the internet possible and plausible to this day. One of the most important cases Moglen defended from arising prosecution was in PGP technology, created by his friend Philip Zimmermann. PGP encryption, standing for “pretty good protection”, is a form of encryption software created by Zimmermann in the dawn of the internet, as a way of sending completely private messages to other individuals on the internet. A very basic understanding of this service is that users of PGP have two “keys” which they use to encrypt and decode messages - a public and a private key. The public key is posted for all to see, which can be used by other users to encrypt messages to you. Once they encrypt and send their message to you, it can only be decoded by the recipients private key. This technology was considered so simple and yet so powerful by the US Military, that they had in effect prevented the technology from being shared outside of national borders, without ever explicitly saying so - they believed this was fair under US export laws surround digital technology at the time. So when Zimmermann exported the information behind the service, the United States government began to prepare a case against Zimmermann and his company. Eben Moglen stepped in to mount a case arguing that the technology was never United States property, and served too important of a purpose in being available to everyone everywhere for privacy protection services on the internet. Within six

months time, the United States dropped their pending investigation against Philip Zimmermann, with Eben Moglen reigning victorious. PGP Encryption technology is still used today, as separate software which can be downloaded and used as a messaging service, or embedded within websites relying on relatively private messaging means. The protection of persecution of PGP technology, ultimately paved the way for modern day remnants of privacy protection on the internet.(Moody 2017) Because of dedicated firms and lawyers like Eben Moglen, users of the internet (at least in the United States) can rest assured that there is devoted dedication towards protecting the freedom of others to use the internet in peace; with the ability to share information and content without critique, obstacles, and oversight - governmental, legal or otherwise - when it comes to the information deemed important and fit to be shared. This legal mindset upholding the defense of total freedom on the internet, is critical towards protecting and growing the legal protections in place for the future availability to use the internet as a place to share information and content deemed important and fit for all; to treat the internet as a true platform of globalized free speech for all.

After carefully reviewing, dissecting, and disseminating all of the research and work I have discussed in this paper, there needs to be a conclusion; a takeaway from the previous research which has either not been said or not been examined in this manner before. My contribution to this new amalgam of theories and research, is a simple concept being proven as a real truth, with each passing day the internet exists in the format it does right now. The internet has become a, if not the, primary source of information channeling in the modern era (for a multitude of different reasons) and while this has opened up channels of communication globally, it has not been without fair appropriation of censorship - at this current point, no country truly has a free and uncontrolled distribution system of information and content; which is okay, as it therefore advocates for a modern, decentralized model of digital existence for people worldwide. This I have defined as a “decentralized individual communications” model, as in theory it would allow and encourage internet users to diversify holding their internet content in

different locations, as opposed to the current system of relying on one predefined set of platforms and providers and therefore “putting all your eggs in one basket”. Internet users should opt to diversify their content to be hosted and provided everywhere in general, regardless of any real or imagined censorship, as it encourages competition for your digital information and media, which will result in greater platform and user control online. An example of this form of decentralization might be where someone who wants to host a taboo or general website, chooses to register their domain name in Russia, while hosting their content online in Germany, or the United States, while discussing risky content in China or anywhere else for that matter. In that way, internet users are protected from a barrage of censorship or any untimely events which may remove their content from visibility online. Regardless of whether this model could or would feasibly work out in a real life scenario, internet users should still consider diversifying their presence online and should become aware of the legal ramifications and protections which are in place to defend or deter users from certain actions and inactions. The longer internet users choose to rely on one system for everything and anything, the worse censorship and curtailing on the internet will get for everyone. Ultimately, recognizing that the internet can never truly be fully “free” and taking steps to at least keep it open and competitive, is the most effective step we can take to retain the internet in the form it currently is in, for as long as possible.

While I studied the ways and means in which people choose to communicate with each other online, I attempted to answer the question of how our digital information and media is controlled and censored in the modern era; I tried to find a way to shine a light on what exactly are the consequences of these actions or inactions, in controlling the flow of digital information. Ultimately I formed the thesis that the internet has become a, if not the, primary source of information channeling in the modern era (for a multitude of different reasons) and while this has opened up channels of communication globally, it has not been without fair appropriation of censorship and control - at this point, no country truly has a free digital distribution of information

and content, which is okay as it therefore advocates for a modern, “decentralized model” of digital existence for people worldwide. This theory is proven relatively true, through all of the sources I choose to use in this paper. Particularly this is true, because I have shown that governments can manipulate the internet, they can control and censor the flow of information, and even without political inference individual users and private companies can “shun” you completely from using their platforms. By the end of my research, I formulated my own perspective on this issue and a few reforms which if taken, could help uphold the free nature of the internet - or a newer digital technology - for a much longer time, without overarching control. My own final view is that the internet has become the main medium for the primary flow of information, the internet has also become woefully threatened by unchecked control, and I recommend that with some legislative and societal changes the internet could become an even more globalized medium, with users functioning in a “decentralized” manner - meaning people have more accounts and platforms in countries all across the globe. If collectively, we all become aware of these ways in which our information is controlled and manipulated, and in effect we take steps to decentralize our presence on certain platforms and our reliance on certain providers, then in due time there is a very real possibility that the “snowballing” damages of greater manipulation and information control on the internet, will be reversed and calmed for an adequate amount of time - at least until the next major technological medium is created or the next digital headache pounces back into court rooms and debate stages across the United States, and the online world. Till then, the internet remains our silver lining sliver of what was once the wild wild world wide web.

Works Cited

1. Heckmann, O. M. (2006). The competitive internet service provider : Network architecture, interconnection, traffic engineering and network design. ProQuest Ebook Central https://ebookcentral-proquest-com.proxy.library.nyu.edu

2. Dinwoodie, G. B. (2017). Secondary Liability of Internet Service Providers: A Comparative Analysis of the Secondary Liability of Online Service Providers Worldwide. Springer Link. https://link-springer-com.proxy.library.nyu.edu/book/10.1007%2F978-3-319-55030-5#editorsandaffiliations

3. Approaches and methods & Histories and pre-histories (2017). In J. Burgess, The Sage handbook of social media. Sage UK. Credo Reference: http://proxy.library.nyu.edu/login?url=https://search.credoreference.com/content/entry/sageukxgxk/approaches_and_methods/0?institutionId=577
4. Social Media's early promise. (2019). In M. L. Issitt, Opinions throughout history: Social media issues. Grey House Publishing. Credo Reference: http://proxy.library.nyu.edu/login?url=https://search.credoreference.com/content/entry/greyothsm/social_media_s_early_promise/0?institutionId=577

5. Ruanne, K. A. (2018, February 21). How Broad A Shield? A Brief Overview of Section 230 of the Communications Decency Act. Congressional Research Service by the United States Congress. https://crsreports.congress.gov/product/details?prodcode=LSB10082

6. Belli, L., & De, F. P. (Eds.). (2015). Net neutrality compendium : Human rights, free competition and the future of the internet : human rights, free competition and the future of the internet. ProQuest Ebook Central https://ebookcentral-proquest-com.proxy.library.nyu.edu

7. Feeney, M., Llanso, E., Perault, M., & Johnson, A. (2021, February 25). If Congress overhauls section 230 to make platforms more liable for user speech, what will change? ITIF | Information Technology and Innovation Foundation. https://itif.org/events/2021/02/25/if-congress-overhauls-section-230-make-platforms-more-liable-user-speech-what-will?mc_cid=f1f3b3a1e5&mc_eid=a51d84e123

8. Kosseff, J. (2019). The twenty-six words that created the internet. ProQuest Ebook Central https://ebookcentral-proquest-com.proxy.library.nyu.edu

9. Wang, J. (2018). Regulating hosting isps' responsibilities for copyright infringement : The freedom to operate in the us, eu and china : the freedom to operate in the us, eu and china. ProQuest Ebook Central https://ebookcentral-proquest-com.proxy.library.nyu.edu

10. Laidlaw, E. B. (2015). Regulating speech in cyberspace : Gatekeepers, human rights and corporate responsibility. ProQuest Ebook Central https://ebookcentral-proquest-com.proxy.library.nyu.edu

11. MIT Technology Review. (2016, November 14). Big data game-changer: Alibaba's double 11 event raises the bar for online sales. https://www.technologyreview.com/2016/11/14/69614/big-data-game-changer-alibabas-double-11-event-raises-the-bar-for-online-sales/

12. Graham-Harrison, E. (2010, July 23). China jails Uighur journalist for 15 years: Employer. U.S. https://www.reuters.com/article/us-china-uighur/china-jails-uighur-journalist-for-15-years-employer-idUSTRE66M1PF20100723

13. Shepard, K. (2020, August 3). An artist stopped posting protest photos online to shield activists from police. Then, he was arrested. The Washington Post. https://archive.md/oiDOP

14. The UnCensored Library. (2020, March 12). The uncensored library – Reporters without borders. The Uncensored Library – Reporters without borders. https://www.uncensoredlibrary.com/en

15. Barrett, P. M., Sims, J. G., & NYU Stern Center for Business and Human Rights. (2021, February). False Accusation: The Unfounded Claim that Social Media Companies Censor Conservatives. https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/60187b5f45762e708708c8e9/1612217185240/NYU+False+Accusation_2.pdf

16. Popper, N. (2018, September 21). PayPal Cuts Off Alex Jones's Infowars, Joining Other Tech Giants. The New York Times - Breaking News, US News, World News and Videos. https://www.nytimes.com/2018/09/21/technology/paypal-blocks-infowars.html

17. LEMLEY, M. A. (2021). The Splinternet. Duke Law Journal, 70(6), 1297–1327

18. TASS Russian News Agency. (2021, February 17). IT exceptionalism? Putin calls out big tech's 'ideological divide', widespread censorship. https://tass.com/politics/1257699

19. Moody, G. (2017, February 21). A lawyer who is also idealist - how refreshing; an Interview with Eben Moglen. the Guardian. https://www.theguardian.com/technology/2006/mar/30/guardianweeklytechnologysection.law

20. Hosseinzadeh v. Klein, 276 F. Supp. 3d 34, 2017 U.S. Dist. LEXIS 134910, Copy. L. Rep. (CCH) P31,140, 2017 WL 3668846

21. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 2000 U.S. Dist. LEXIS 11862, 55 U.S.P.Q.2D (BNA) 1780, Copy. L. Rep. (CCH) P28,126

22. Golding, B. (2021, January 14). Curt schilling says AIG canceled insurance over his social media posts. New York Post. https://nypost.com/2021/01/14/curt-schilling-says-aig-canceled-insurance-over-social-media-posts/

23. Scott, T. (2020, March 23). YouTube's Copyright System Isn't Broken. The World's Is. YouTube. https://www.youtube.com/watch?v=1Jwo5qc78QU