(1)Several authors such as Stallman and Barlow are against the use of software patents due to several arguments. One of these arguments is that software is not something that is tangible, as it is not something that can be held or touched like physical properties. Not only that, unlike physical property, the exact same software can be owned by many people at the same time instead of only one person at a time. Intellectual properties are also different from physical property due to the fact that they are never in a fixed state; they can be changed at any point in time. Scarcity does not determine IP’s value and IP in software changes too drastically to be owned with any patents. For example, if you’re copying a computer software from someone, the owner will still have the software, therefore, it should not be considered an act of theft.

The arguments that these authors form do not show that software patents should be eliminated. This is because some of these authors are arguing for the patent process to not be completely taken out, but instead revised into a more suitable way of patenting. For example, instead of patenting just a chunk of code or software, the entire program as a whole should be patented. For example, we cannot just patent all the nodes or tones or usage of certain musical instruments. Instead, we should patent the song as a whole, because similar nodes, tones or usage of musical instrument doesn’t mean that they are copying the song. This applies directly to the argument of patenting the entire application instead of the algorithm and code. While they are upset about how the current patenting system works, they don’t necessarily want them completely off the table because of how patents have the potential to protect ideas. Furthermore, patents are very costly and the process to get the patent approved are way too long, causing the smaller companies to be unable to get patent.

The mathematics and logic behind algorithms are sometimes unaware, thus there are multiple patents of the same algorithms but serves different purposes. Example, IBM issue a patent on the same algorithm that Unisys supposedly owns, the two patents have the same algorithm but different descriptions even though the formulas are mathematically equivalent. Software patents does not discourage trade secrecy as it was normal for computer scientist in commercial as well as academic to publish their discoveries which shows secrecy about techniques was not a significant problem. Thus, little to gained by adopting the patent system to discourage it. Utilitarian: Removing software patents would produce the greatest net benefit as time is not wasted in requesting and getting a patent approval, instead the time can be used productively in improving and producing quality algorithms which promotes innovations. Plus, removing patents saves money as small or large company does not need to worry about purchasing rights to a patent nor receiving a patent lawsuit, thus the money saved can be used in carrying out events like Hackathon that educates the young generation about computer programming as they are the main source of future innovations. However, IP rights provide motivation incentives for creating and developing better goods. If intellectual property rights are not protected no one will take the trouble to develop programs and patents and so on, thus potential programmers will be poorer consequently.

(2) There are several points to the “hacker ethic” by Denning. First, it states that exploratory hacking promotes a greater distribution of information. This means that any useful information should be free for everyone, helping in educate the society. Denning also claims that, by hacking helps promote the spread of information and knowledge to the society, which helps building a smarter and more knowledgeable society. She suggests that all information should be free to the public just like public libraries, so anyone can access your system to look for information. She also states in the hacker’s ethic that exploratory hacking helps in revealing the weaknesses of a certain system. The hacker will then reveal the security breaches to get attention from everyone. On her last point in the hacker ethic, she said that exploratory hacking work as a kind of public policing to make sure government and public companies aren’t misusing and exploiting confidential information. //The main claim that an exploratory hacker makes is that they are only hacking just to obtain knowledge from computer programs. Not only that, they also say that they have no intention of causing any damage or harm to the system that they’re exploring, or to access any form of private information that they aren’t supposed to know, such as account passwords or credit card information. However, I personally believe that exploratory hacking is morally impermissible. My view is mainly influenced by a utilitarian view, as I believe that exploratory hacking would cause more harm than good to the many people involved. Extending from that, I also believe that exploratory hacking is not morally right according to the Categorical Imperative of Kantian Ethics as well, because one should avoid harming others altogether.  The hacker’s actions are morally wrong as they are still infiltrating private information, regardless of intention. //First, these exploratory hackers are hacking into systems that they may not fully know what sort of information they would stumble on. Take the incident of the recent Facebook password scandal that occurred on the 21st of March 2019, for example. According to CNN, hundreds of millions of users’ passwords were stored as plain text instead of being masked and protected with a layer of encryption. Now, let’s assume that an exploratory hacker was to hack Facebook’s programs with the notion in mind that they wouldn’t knowingly stumble on any private information such as account passwords. They would be wrong as the passwords are already laid out in the open without any form of encryption, free for all to see. Even though it isn’t their fault that the information was not well protected, they still are responsible because they were hacking into a system that they aren’t allowed in. Consequently, this puts many users in a potentially harmful situation as there is someone out there who knows the passwords to their accounts. Based on the utilitarian perspective which says that there should be a greater good for a greater amount of people, I believe that the harm done on hundreds of millions of users greatly outweigh the good of one, or a team of exploratory hackers who are just hacking to gain knowledge. //Another reason why I believe exploratory hacking is wrong is because there are other people who the hackers may be harming unknowingly as well. While they claim that they don’t have the intention to harm the systems that they are exploring, there still is the possibility where they may unknowingly break some parts of the program.  The process of hacking alone could cause irreparable harm to the security system and may leave the data of the users in jeopardy if a non “altruistic” hacker should decide to maliciously steal information. // The criticisms of Eugene Spafford are mainly constructed against the “hacker ethic”. He strongly disagrees exploratory hacking. Even though exploratory hacking may sound good on the surface, but that also allow hacker to have the full access to the system which may possibly lead to extremely dangerous consequences.// It is also stated in the hacker’s ethic that one of the main points of exploratory hacking is that it leads to a greater distribution of information. This may sound really good and positive, but there’s certain information that are preferably kept private. For example, banking information, medical information, and home address should be kept private as it could easily be misused by the hacker. Spafford also claims that we would lose all the sense of privacy and property if the all the information were to be free and can be accessed by anyone. I think it is too naïve to think that all information will be used ethically if the any information is easily reachable. // Spafford also disagrees with the second main point of Denning’s hacker ethic is that hacking into someone’s systems to learn about their systems. Spafford argues that people cannot take the system apart just to learn about how the system works, even though on the surface may look like there is not damage that is done to it, but the system will never be the same. For example, dissecting an animal to learn about the organs in the body, but when you cover the part up, it will still leave a scar on the skin, so no matter how minor the changes are, it is still not original anymore. --Another one of the fundamental points of the “hacker ethic” states that a hacker could infiltrate a system in order to test the security, but Spafford argues that a problem does not need to be tested in such a drastic way in order to be identified.  Spafford says that computer systems are resources, and they are not meant to be exploited to play with security. Not only that, he also makes the claim that the owners of these computer systems should not be held responsible for every single security flaw found in their programs--Lastly, the act of hacking into a system without the administrator’s express permission is unethical and immoral.  If hackers are allowed to hack into systems, who is to stop them when they hack with less ethical intentions? Criminal activity could be confused with commendable behavior, allowing criminals to get away with crimes.

This paper will be primarily focused on the various problems stemming from the censorship of materials found on the internet. Extending from that, it will discuss the author’s opinions on the best possible way for regulation of posts on the internet. Finally, this paper will elaborate on the author’s views regarding who should be held responsible for the regulation of online content.

Censoring materials online can be the root cause of many different problems. Take the case of the recent Tumblr censorship which occurred in December of 2018 as an example. According to Powell, due to the new censorship regulations released by the CEO of Tumblr Jeff D’Onofrio on the 3rd of December, safe spaces for the underrepresented groups such as women and the LGBTQ community are destroyed. Powell also takes a jab at tech corporations who all claim to want to create a safe haven for diverse communities but destroying it at the same time (Powell, 2018). Furthermore, censoring content online as Tumblr did isn’t necessarily the wisest decision either. In an article by The Verge, it writes that almost thirty percent of all of Tumblr’s traffic has dropped due to the censorship (Liao, 2019).  Besides, according to firsthand experience, the author would like to note that soon after the censorship of Tumblr took place, part of the community who were upset with the restrictions found themselves moving to a newly made website named “bdsmblr.com”, a sexually explicit version of Tumblr, thus making the censorship ineffective in a way.

A different problem that

//EXTEND FURTHER write about a different problem, Net Neutrality

With all of these problems arising from censorship, we should strive further and seek better ways to perfect the censoring process. Basing off on the four modes of regulation by Larry Lessig, which are: the Law, the Market, the Code, and Social Norms, the author believes while social norms would be the most effective in regulating content, a combination of all four is still needed to produce the best process of censorship. The author’s views on these modes will be elaborated further in the next few paragraphs.

Using laws to regulate the internet can prove to be tricky, as depicted in the case of the “ILOVEYOU” virus of May 2000. According to Knight, the creator of this virus named Onel De Guzman who was found to be in the Philippines was not prosecuted for the damage they had done internationally as there were no existing laws in the Philippines at the moment for a case such as this. Instead, Guzman was only charged for credit card fraud which was part of what the ILOVEYOU virus did (Knight, 2000). As such, the author believes that there should be more substantial international laws on the internet in place before we can turn to these laws and rely on them as regulation.

The author believes that the Market, on the other hand, is one of the weakest ways to regulate a website. This is because there will always be companies who will willingly post advertisements on a website no matter how morally ambiguous or wrong a website may be. The website which I’ve mentioned earlier, “bdsmblr.com” has advertisements supporting it, just like how “PornHub” has them too. As such, a Market driven censorship regulation does almost nothing at all. Taking a different perspective of Market driven regulation, the author would like to reuse the same Tumblr example as used earlier in this paper. Forbes reports that one of the main reasons why Tumblr released their recent censorship policies was due to the fact that their app was removed from the Apple App Store in November of 2018 due to sexual images of children found on the site. (Sands, 2018). Of course, with one of the major application stores not supporting a website’s app, it only makes sense that the website would have to rethink its decisions and choices in order to redem itself from this Market-driven pressure. Although this may be a good example of how the Market can positively affect censorship regulations, but as discussed earlier, these regulations were almost ineffective due to how the situation was handled.

Code is a form of regulation which the author believes works better than both the Law and the Market, although it still isn’t the best. In an article written by Fan Yang in 2016 for the journal “New Media & Society”, it talks about the Chinese government has set up filters in their code to help filter out words that are deemed to be against their repressive regimes, extending so far to even censor out words which are homonyms to the actual words (Yang, 2016). However, at the stage of technology in which we are at now, code and algorithm are still unable to completely carry out the censorship the way China wishes it to be. This is because humans are still able to be creative and come up with more ways to go around the code. For example, in Yang’s paper, it also talks about how people on the internet kept evading the “Great Firewall” by endlessly creating new terms which get more and more inconspicuous. One such example would be how the Chinese netizens eventually came up with a term, “UA989”, to refer to a blind man who was arrested in America.  Not only that, Chinese netizens could also use a VPN (Virtual Private Network) in order to overcome this firewall of censorships which the Chinese government has set up (Yang, 2016).

When it comes to the social-norm, the author believes that it is the best way to regulate content due to several reasons. First of all, should there be a post on a website such as Facebook which consists of immoral or banned material, the users who see it can report it to Facebook so that their administrators could look into it and make sure that it really is unwelcome content. It’s not only Facebook that has this feature. The major video sharing site, YouTube, has a flagging system, and another giant social media platform, Twitter also has a report function. Both of these work the same way as Facebook does, where they all rely on the community to give feedback on what could be deemed as unwelcome as according to their policies. Just as discussed in class regarding the case of the website, AutoAdmit, where its adamant standing on being unmoderated caused it to have a bad reputation, it is clear that there should be some form of social-norm regulations whether it be having administrators or having the community of the website work together to form a safe space for all (Tsou, 2019).

With that said, all the different modes of regulation could still work hand in hand to help create a much better way to regulate the internet and what is being posted on it. First of all, the author proposes that instead of prosecuting criminals who use the internet to do heinous activities based on their own nation’s laws, we should have a set of laws that could regulate the entire internet world. This proposal would be akin to having the internet be treated as if it is it’s own country, with its own set of laws. This is because without these universal laws, there could be potential criminals out there causing harm to others via the internet but not getting the punishment that they deserve as there are loopholes in the current law system. Although it is not ideal due to capitalism, we could also use the market as a regulation mode by having //WTF In addition to the structure that those two modes of regulation, code could be used as an extra layer of regulation in order to further enhance the censoring process. For example, by using algorithms, we can effectively scan through user input for materials which are deemed unsafe for the community then blocking such materials from getting on the internet on the first place. Of course, these algorithm won’t always work perfectly. There will always be some indecent material slipping through the walls of code. Likewise, there may also be perfectly fine material that would be wrongfully deemed unsafe to pass through by those algorithms. In these cases, regulation by social norm can be added on to fortify the regulation process. The administrators could be notified about these mistakes by the users and consequently make the right amends. The author suggests this as a last resort for two reasons. One, this would be the most cost effective way of working through the problem of regulation, as the websites would have to hire less people to help with administration regulations. Two, as some material which are trying to pass through the code wall may be unsettling and can cause psychological damage to the administrators over extended exposure, it would be safer for the administrators to be exposed to the least amount of such material as possible.

In a way, the author believes that everyone should be held responsible for the regulation of the contents on the interne