Name(s)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Period \_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
|  | **Project Guide - Internet Dilemmas** |  |

## Background

You are the Chief Technology Advisor for a candidate running for elected office. Your candidate is relying on you to help inform her about important technological dilemmas and come up with good policy ideas to address them. For this project you’ll investigate a social dilemma related to the Internet and prepare a report summarizing your findings and making a policy recommendation for your candidate.

## Step 1 - Pick Your Dilemma

|  |  |  |
| --- | --- | --- |
| **Net Neutrality** | **Internet Censorship** | **The Digital Divide** |
| **Background:** Internet users love services like streaming movies, video chatting, or online gaming. All of this content needs to travel over the Internet, however, and the companies that build and maintain networks are complaining about the increased demands being placed on their networks. Your candidate is hearing more and more about a debate called “net neutrality” and would like a more informed opinion as part of her platform. | **Background:** While the Internet is used to share many useful services and information, there are growing concerns about the way that the Internet can be used to spread damaging information ranging from national secrets to calls for violence. Censoring this information may provide some people with increased security, but potentially risks free speech and the safety of social and political activists. Your candidate would like to have a policy that balances these two concerns in a way that makes sense for our digital age. | **Background:** While technology is increasingly integrated into daily life, there are still many who lack access to the Internet or digital technology. In rural areas there are challenges building networks to connect geographically sparse populations, but even in cities some groups or areas have relatively less access to the Internet or knowledge of how to use it. Your candidate is worried that while technology is bringing social and economic benefits to many, there are others being left behind. |
| **Core Question:** When and how should internet service providers be allowed to treat some kinds of internet traffic different from others? | **Core Question:** When and how should the government be allowed to censor or block internet traffic, if at all? | **Core Question:** When and how should resources be invested to close gaps between those who do and don’t use the Internet? |
| **Impacted Groups**   * Internet Service Providers (ISP) * Internet Content Provider * Everyday internet Users | **Impacted Groups**   * Everyday internet user * Intelligence Agencies * Political activists | **Impacted Groups**   * Those lacking internet access * Internet Service Providers (ISP) * Schools and libraries |
| **Sources**   * "How the end of net neutrality could change the internet" (video): [link](https://www.youtube.com/watch?v=HqXKEgTYZBQ) * "'Net Neutrality' is ending. Here's how your internet could change" (article): [link](https://www.pbs.org/newshour/nation/net-neutrality-is-ending-heres-how-your-internet-use-could-change) * "Wikipedia - Net Neutrality": [link](https://en.wikipedia.org/wiki/Net_neutrality) | **Sources**   * "Free Speech Or Hate Speech: When Does Online Hate Speech Become A Real Threat?" (audio article): [link](https://www.npr.org/2018/11/19/669361577/free-speech-or-hate-speech-when-does-online-hate-speech-become-a-real-threat) * "Internet Censorship Explained" (video): [link](https://www.youtube.com/watch?v=6ohH-RkSLo4) * Wikipedia - Internet Censorship: [link](https://en.wikipedia.org/wiki/Internet_censorship) | **Sources**   * "Eliminating the Digital Divide" (video): [link](https://www.pbs.org/video/eliminating-digital-divide-ihdcln/) * "Internet/Broadband Fact Sheet" (article): [link](https://www.pewresearch.org/internet/fact-sheet/internet-broadband/) * Wikipedia - the Digital Divide: [link](https://en.wikipedia.org/wiki/Digital_divide) |

## 

## Step 2 - Review the One-Pager and Rubric

Review the one pager template and rubric to make sure you understand what you’ll be responsible for creating for this project and how it’ll be evaluated.

I did this

## Step 3 - Review the Concept Bank

This concept bank includes the key terms and concepts covered in this unit. Quickly review them before reading your articles so that you’ll be ready to identify them in your articles. You can also refer to these as you complete your one-pager.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Protocols / Layers**  Physical internet, IP, TCP, UDP, HTTP, DNS | **Networks**  Fiber optic cable, copper wire, wifi, router, path, direct connection, bandwidth | **Packets and Routing**  Packet metadata, IP addresses, dynamic routing, | **World Wide Web**  Web pages, browsers, servers, domain, world wide web | **Internet Principles**  Redundancy, fault tolerance, scalability, open protocols |

## Protocols / Layers:The internet comprises many layers and protocols that all work together to move information around a network of devices. Each protocol builds upon the last creating layers with higher layers relying on the ones below them.

## Networks: Networks are the physical connecting of one device to another, and information can travel through the system. Computers do not need to be directly connected; computers only need to be connected via a single point on the network.

## Packets and Routing: With the help of the Internet Protocol, Transmission Control Protocol, User Datagram Protocol, Domain Name Systems, and the HyperText Transfer Protocol, a system can route packets over a physical network and the World Wide Web. The Internet Protocol assigns an IP address to every router on the network and every device connected to said router. For someone to access a website, they must call upon HTTP, which allows computers to request and share data; this is the World Wide Web. Before someone can use HTTP, they must first send TCP/IP packets to a Domain Name System. TCP/IP Packets are for a message to be sent all at once; error checking will take place, making TCP more reliable but slower than UDP, and a Domain Name System translates a domain to the domain's IP address allowing HTTP to happen.

## World Wide Web: For someone to access a website, they must call upon HTTP, which allows computers to request and share data; this is the World Wide Web.

## Internet Principles: Transmission Control Protocol, Internet Protocol, User Datagram Protocol, Domain Name System, HyperText Transfer Protocol, Uniform Resource Locator, Domains, sockets, ports, and more all work together to check for redundancy and fault tolerance. They all also allow the internet to be scalable; for example, DNS helps the internet scale by enabling billions of users to access billions of domains. DNS servers talk to other DNS servers; this means that only 1 DNS server has your domain and IP address. That is the big takeaway. DNS servers communicate with/to other DNS servers, allowing billions of users to access billions of web pages, allowing the internet to scale.

## Step 4 - Review Your Sources

Review the three sources provided or additional ones you find online. For each source take notes on instances when your impacted groups are mentioned or technical details are explained.

|  |  |  |
| --- | --- | --- |
| [**Source**](https://www.npr.org/2018/11/19/669361577/free-speech-or-hate-speech-when-does-online-hate-speech-become-a-real-threat) | **Notes on Impacted Groups** | **Notes on Technical Details** |
| [NPR](https://www.npr.org/2018/11/19/669361577/free-speech-or-hate-speech-when-does-online-hate-speech-become-a-real-threat)  [Free Speech Or Hate Speech: When Does Online Hate Speech Become A Real Threat?](https://www.npr.org/2018/11/19/669361577/free-speech-or-hate-speech-when-does-online-hate-speech-become-a-real-threat) | * Families and Friends * Minorities * Extremists * Rochelle Ritchie * Andrew Torba * Jonathan Rauch * Facebook & Twitter   Rochelle Ritchie was tweeted at by a political commentator, saying, "kiss your loved ones when you leave home." A few weeks later, somebody accused Rochelle Ritchie's tweeter of sending over a dozen explosive devices nationwide.  Andre Torba thinks that censorship and pushing people into the shadows isn't going to be the answer. He believes that guns and social media platforms don't kill people; people kill people.  Jonathan Rauch believes that fighting hate by repressing hate speech is like trying to deal with global warming by breaking thermometers. He thinks that the problem is not speech, but hatred and the only way to deal with the problem is by confronting it. | There is a disconnect between hate speech and free speech. The supreme court said that hate speech is generally protected under the constitution.  Even if something is hateful, that won't cause any real threat. People kill people, not ideas that people have. If someone does not act upon those ideas, then nothing will ever happen.  Confronting hate speech is key to the advancement of civil rights in America.  Facebook is taking additional steps by monitoring content complaints.  The First Amendment prevents government censorship.  Private social media companies like Facebook and Twitter can do whatever they want. |
| [Computerphile](https://www.youtube.com/watch?v=6ohH-RkSLo4)  [Internet Censorship Explained - Computerphile](https://www.youtube.com/watch?v=6ohH-RkSLo4)  as well as  [Computerphile](https://www.youtube.com/watch?v=nqbyS_Z74nc)  [EXTRA BITS – Internet Censorship- Computerphile](https://www.youtube.com/watch?v=nqbyS_Z74nc) | * User * Publisher * Twitter * Facebook * Censor * Muslim countries * China   Users and Publishers are in the middle of censorship and censorship resistance. This censorship resistance is called coercion of users or coercion of publishers, and it is how anonymous or untraceable one can be. Ideally, one of the goals of a comprehensive censorship resistance system is to afford that kind of privacy to users, but they usually do not do that kind of thing.  Facebook and Twitter have loads of user-generated content, and it is challenging for a censor to retain control of that information.  There is an extensive range of reasons why a censor might want to censor information. A censor might like to edit information because of religion, hate speech, privacy, security, political, temporary political. For example, during an election, one candidate could block access to another website during the election period.  Most Muslim countries block access to pornographic content.  China might have an underlining motive, but China desires to control the information users can access in their country.  China has local alternatives to Google and Facebook, and other popular social media. | The critical point of internet censorship is to stop the information sent between a user and a publisher from being disseminated.  Internet censorship comprised a range of steps that the censor might take to either stop the publication of information on the publisher’s side or discourage access to that information.  DNS redirection or DNS sinkholing is a way censorship could happen. DNS sinkholing occurs when the user using a browser to send an HTTP Get Request for a domain to a Domain Name Server for some index page of their desired website. Still, the censor could block the user’s connection at the DNS level and redirects them to a new IP.  IP blocking is the blocking of an IP address.  When accessing any site, somebody can trace you.  Tor is an anonymity service that can help decensor sites.  China’s censorship gives a boost of money to local companies in terms of discouraging computation.  Most countries that censor their people install software called censorship resistance systems. |
| [Wikipedia](https://en.wikipedia.org/wiki/Internet_censorship) [Internet censorship](https://en.wikipedia.org/wiki/Internet_censorship) | * Facebook * Google * Twitter * Youtube * Wikipedia * Yahoo! * Lèse majesté sites * Falun Gong and Tibetan exile groups * 50 Cent Party / 50 Cent Army * China * Russia * Christianity * Islam * LGBTQ+ * Pro -North Korean sites * WikiLeaks * 4Chan * Muslim Brotherhood   Facebook's statement of rights and responsibilities says that you cannot post anything that "is hateful, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence," and Facebook says that they have the right to remove any content or information you post on Facebook if they believe that it violates their statement of rights and responsibilities.  Google and Google Search both state that they have the right to suspend or stop providing services to their users if they do not comply with their terms or policies or under investigation. Google Search says that they have the right to temporarily or permanently remove sites from their index and search results if they believe it did not meet their quality guidelines or for other reasons.  Twitter's terms of service state that they reserve the right at all times to remove or refuse users' posts or reclaim usernames.  There could be security concerns for Pro -North Korean sites, WikiLeaks, 4Chan, and Muslim Brotherhood sites. | Internet censorship controls or suppresses what can be viewed, published, accessed, or changed on the internet. Internet censorship is controlled by regulators or by individuals and organizations that engage in self-censorship.  Some democratic countries have moderate Internet censorship, and other states limit access to information like citizens' news.  In a 2012 Internet Society survey, 71% of respondents agreed that censorship should exist on the internet in one way or another, 83% agreed that access to the internet should be a fundamental human right, and 86% agreed that freedom of expression should be guaranteed on the internet.  Blacklists can be produced manually or automatically.  Parties can use different technical methods of preventing public access to information.  There are many different approaches to censoring the internet. This included IP address blocking, DNS filtering and redirection, URL filtering, packet filtering, connection reset, network disconnection, portal censorship, search result removal, computer network attacks, denial of service attacks, over and under blocking, use of commercial filtering software, and more.  Governments and other organizations don't want citizens to know their dark secrets and try to use censorship to cover them. |
| [Harvard](https://cyber.harvard.edu/pubrelease/internet-control/) [Internet Censorship and Control](https://cyber.harvard.edu/pubrelease/internet-control/) which referenced  [King-wa Fu, C.H. Chan and Michael Chau  Assessing Censorship on Microblogs in China: Discriminatory Keyword Analysis and Impact Evaluation of the “Real Name Registration” Policy](https://poseidon01.ssrn.com/delivery.php?ID=321102020088086120082091100031096069021063020068087078105086030089003091108098125119059058002121107109114088099100071115088023050009068002021112001120106031008118029090058030123026097119025078127069068077086117093027109003101011119003087094094066086114&EXT=pdf) | * China * Chinese citizens * Mail providers (ProtonMail and Tutanota)   China has an extensive and explicit censorship infrastructure that can interact with the rest of the internet.  Total Chinese Internet users reached 538 million by mid-2012 (40% of the country’s population).  Webmail providers are using HTTPS encryption is to allow access to their services and help users avoid monitoring by their governments.  ProtonMail and Tutanota use more intense encryption than just HTTPS. Tutanota uses the same algorithms as PGP – AES, and RSA to encrypt emails. Tutanota is also published on GitHub to ensure that security experts can check and see no encryption backdoors. | The internet protocols TCP and IP are two core protocols that define the internet. They both are designed to allow different networks to interact with each other easily. They are designed for this so that networks differ in both hardware implementation and their politics of control.  According to the China Internet Network Information Center (CNNIC): By 2012, 51% of the total Internet population was Chinese microbloggers.  A vulnerability of Certification Authorities responsible for establishing HTTPS to sites is that certification authorities can impersonate any website to any user. This power has made Certification Authorities a significant target for hackers. |

Name(s)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Period \_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
|  | **Internet Dilemma Policy One Pager** |  |

***To complete this one pager fill in each of the sections below. All text in italics is included to explain how to fill in the one pager and can be deleted before you submit.***

## Core Question

When and how should the government be allowed to censor or block internet traffic, if at all?

## Impacted Groups

|  |  |
| --- | --- |
| **Impacted Group and Description** | **Interests, Benefits, and Harms** |
| China and Chinese citizens:   * China has local alternatives to Google and Facebook, and other popular social media. * China can spy on every citizen and track them through their mobile applications. * China is the world’s most populous country, with around 1.4 billion citizens. * China’s Internet censorship is more extensive and advanced than any other county in the world. * More than 60 online restrictions have been made by the Government of China, which have been implemented by state-owned ISP companies. | * China desires to control the information its citizens can access in their country. * Chinese citizens want to view censored data, but the Chinese government won't let me. * China can benefit from censorship since it can control its citizens, but they can also be harmed by citizens fighting back in forms of protests, riots, or immigration. * Chinese citizens can benefit by not knowing everything that is happening in the world because ignorance is bliss, but they can also be harmed by getting controlled by the government. * Chinese citizens are not able to do anything against the rule of the government. * Chinese citizens are interested in VPNs, proxies, tor, and other ways to go around the government firewall to obtain information. |
| Social Media Companies (Facebook, Twitter, YouTube, Snapchat):   * Social media are web-based sites that allow people to interact with each other, including family and friends. * Social media usually consist of personal user accounts, profile pages, friends, followers, groups, hashtags, newsfeeds, personalization, notifications, information updating, saving or posting, like buttons, comment sections, reviews, rating, or voting systems, and more. * Some social media companies are/were Facebook, Instagram, Snapchat, Twitter, YouTube, TikTok, Vine, Tumblr, Linkedln, WhatsApp, Pinterest, Reddit, Mix, Twitch, Mixer, and of course, the list goes on. | * These groups' interests are to 1 make money and 2 to provide a platform where people can connect and be a part of a community. * The benefits of having a platform where people can connect are huge. People can learn, relax, make friends, find their loved ones, get a girlfriend/boyfriend/wife/husband, enjoy life, improve their health, get help, and more. * With a long list of benefits comes a long list of potentially harmful things. People can choose to be anonymous on these social media platforms, and they can create chaos. People can influence others to break the law, end their lives, and end others' lives or experiences; they can spread misinformation, hack others, spread hate speech, and more awful things. * The result of social media platforms is directly proportional to the amount of wrong on the site. If there are more hateful messages than good ones, this will lead to a toxic platform that can harm. * Social media users can benefit from censorship when it has to do with hate speech or offensive content and nudity. * Social media users can get harmed from censorship because information, including the truth, could be covered up, plagiarized, and lost. |
| Muslims:   * People who follow the Islam religion. People who accepts surrender to the will of Allah, pray, and read the Quran. * Many Muslims live in the middle east like citizens who live in the UAE. * Muslims pray 5 times a day and follow srict rules to protect themself against haram (very forbidden activities, like sins and the commandments in the christian religion). | * Muslims believe that God has mercifully given guidance to humankind that they all must follow it. * A Muslim wants only what is best for them and their brothers; Muslim brotherhood is essential. * Muslims are often seen as terrorists and, therefore, are censored for anything they do and say. Muslims would benefit from not being edited because most Muslims do not believe in what terrorists have done. Somebody should censor the small fraction of radical Muslims who are terrorists because they can do more harm than good if they aren't. * Muslims are harmed by censorship but also benefit from it in some instances. The large population of Muslims is hurt from censorship more often than they benefit from it. Muslims are harmed by censorship because it creates political tension when they are wrongfully censored, leading to worse things. |

## Technical Background

The technical background necessary to understand when and how the government should be allowed to censor or block internet traffic if at all, comes down to a few layers, protocols, and principles of the internet. First, let's understand what internet censorship is. Internet censorship controls or suppresses what can be viewed, published, accessed, or changed on the internet. Internet censorship is controlled by regulators or by individuals and organizations that engage in self-censorship. There are many different approaches to censoring the internet; this includes IP address blocking, DNS filtering, and redirection, URL filtering, packet filtering, connection reset, network disconnection, portal censorship, search result removal, computer network attacks, denial of service attacks, over and under blocking, and use of commercial filtering software. With the help of the Internet Protocol, Transmission Control Protocol, User Datagram Protocol, Domain Name Systems, and the HyperText Transfer Protocol, a system can route packets over a physical network and the World Wide Web. The Internet Protocol assigns an IP address to every router on the network and every device connected to said router. For someone to access a website, they must call upon HTTP, which allows computers to request and share data; this is the World Wide Web. Before someone can use HTTP, they must first send TCP/IP packets to a Domain Name System. TCP/IP Packets are for a message to be sent all at once; error checking will take place, making TCP more reliable but slower than UDP, and a Domain Name System translates a domain to the domain's IP address allowing HTTP to happen. With the basics out of the way, DNS redirection or DNS sinkholing is a way censorship could happen. DNS sinkholing occurs when the user using a browser to send an HTTP Get Request for a domain to a Domain Name Server for some index page of their desired website. Still, the censor could block the user's connection at the DNS level and redirects them to a new IP. Many groups are affected by internet censorship, including all citizens of basically every country. Some democratic countries have moderate Internet censorship, and other states limit access to information like citizens' news, like China. China has an extensive and explicit censorship infrastructure that can interact with the rest of the internet.

## Recommended Policy Solution

|  |  |
| --- | --- |
| **Recommended Policy:** The government should not be allowed to censor or block internet traffic of their law-abiding citizens. The only time the government should be allowed to censor or block internet traffic is when people's lives are in danger. All companies are still able to make their own terms of service rules. | |
| *Pros / Who Benefits*   * Every citizen benefits since every citizen can now see the real truth of what is happening in today's society. * Social media companies benefit from this because they do not need to change anything they have worked hard to make. * Religious groups that have been wrongfully censored benefit because they can spread their religious beliefs more easily. | **Cons / Who is Harmed?**   * Corrupt governments are harmed because they cannot censor important information that could be helpful for their citizens to know. * Terrorists are harmed because they will get censored, and no one will see their messages. * Citizens subjected to racial slurs and discrimination are still harmed because this policy doesn't change hate speech law. With this policy, hate speech is still free speech. |

## 

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Extensive Evidence** | **Convincing Evidence** | **Limited Evidence** | **No Evidence** |
| Completed research guide demonstrates use of multiple sources | Research guide indicates referencing three or more sources. provided are referenced | All three provided sources are referenced | Only one or two sources were referenced | No evidence that sources were used |
| Interests, benefits, and harms of all impacted groups are clearly explained | Interests, benefits, and harms for all groups, including possibly additional groups beyond the required three, are provided. | Interests, benefits, and harms of most groups are provided and accurate. | Interests, benefits, and harms are either limited, inaccurate, or incomplete. | No description of impacts on different groups |
| Technical details reflect an accurate and detailed understanding of the internet | Extensive technical details are provided demonstrating broad understanding of how the internet works | Many technical details are provided that accurately reflect how the internet works | Few technical details provided. Some may be inaccurate. | No technical details provided |
| Technical details are clear and described for a non-technical audience | All technical details are clear and easily read by a non-technical audience | Most of the technical details provided can be understood by a non-technical audience | Many of the technical details provided are confusing to a non-technical audience | No technical details provided |
| A clear policy recommendation is provided that is justifiable based on other information in the one-pager | Policy recommendation is justifiable and clear based on information in both other sections of one-pager | Policy recommendation is clear but some aspects may not build upon information elsewhere in the one-pager | Policy recommendation provided but is disconnected from other information in one-pager | No policy recommendation provided |
| Reasonable benefits and harms of the policy choice on different impacted groups are provided | Benefits and harms to all impacted groups are clearly explained | Benefits and harms to most impacted groups are clearly explained | Benefits and harms are limited or not tied to specific groups | No benefits and harms are provided |

Short Summary Essay:

When and how should the government be allowed to censor or block internet traffic, if at all?

I believe that the government should not be allowed to censor or block internet traffic of their law-abiding citizens. The only time the government should be allowed to censor or block internet traffic is when people's lives are in danger. All companies are still able to make their terms of service rules. I believe this because when it comes down to it, the government controls everything you see and everything you can access when you are on the internet.

Internet censorship controls or suppresses what can be viewed, published, accessed, or changed on the internet. Internet censorship is controlled by regulators or by individuals and organizations that engage in self-censorship. There are many different approaches to censoring the internet; this includes IP address blocking, DNS filtering and redirection, URL filtering, packet filtering, connection reset, and network disconnection. There is also portal censorship, search result removal, computer network attacks, denial of service attacks, over and under blocking, and commercial filtering software. With the help of the Internet Protocol, Transmission Control Protocol, User Datagram Protocol, Domain Name Systems, and the HyperText Transfer Protocol, a system can route packets over a physical network and the World Wide Web. The Internet Protocol assigns an IP address to every router on the network and every device connected to said router. For someone to access a website, they must call upon HTTP, which allows computers to request and share data; this is the World Wide Web. Before someone can use HTTP, they must first send TCP/IP packets to a Domain Name System. TCP/IP Packets are for a message to be sent all at once; error checking will take place, making TCP more reliable but slower than UDP, and a Domain Name System translates a domain to the domain's IP address allowing HTTP to happen. With the basics out of the way, DNS redirection or DNS sinkholing is a way censorship could happen. DNS sinkholing occurs when the user using a browser to send an HTTP Get Request for a domain to a Domain Name Server for some index page of their desired website. Still, the censor could block the user's connection at the DNS level and redirects them to a new IP.

Many groups are affected by internet censorship, including all citizens of basically every country. Some democratic countries have moderate Internet censorship, and other states limit access to information like citizens' news, like China. China has an extensive and explicit censorship infrastructure that can interact with the rest of the internet. Suppose the policy that I suggested earlier comes into place, then every citizen benefits since every citizen can now see the real truth of what is happening in today's society. Social media companies benefit from this because they do not need to change anything they have worked hard to make, and religious groups that have been wrongfully censored benefit from spreading their religious beliefs more easily. In a 2012 Internet Society survey, 71% of respondents agreed that censorship should exist on the internet in one way or another, 83% agreed that access to the internet should be a fundamental human right, and 86% decided that somebody should guarantee freedom of expression on the internet. I believe this to be true, and to uphold the public opinion on this matter, we need to remove censorship on everything that isn't terrorism.

I leave you with my recommended policy: The government should not be allowed to censor or block internet traffic of their law-abiding citizens. The only time the government should be allowed to edit or block internet traffic is when people's lives are in danger. All companies are still able to make their terms of service rules. My policy will help many and only harm corrupt governments like china and terrorists. Corrupt governments are harmed because they cannot censor important information that could help their citizens learn, and terrorists are hurt because they will get censored, and no one will see their hate messages.