Name(s) sharena sharif   Period 5, 6   Date 11/13/23

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 ● "'Net Neutrality' is ending. Here's how your internet could change" (article): link ● "Wikipedia - Net Neutrality": link	**Sources** ● "Free Speech Or Hate Speech: When Does Online Hate Speech Become A Real Threat?" (audio article): link ● "Internet Censorship Explained" (video): link ● Wikipedia - Internet Censorship: link	**Sources** ● "Eliminating the Digital Divide" (video): link ● "Internet/Broadband Fact Sheet" (article): link ● Wikipedia - the Digital Divide: link

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.

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

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	Notes on Impacted Groups	Notes on Technical Details
● Wikipedia - Internet Censorship: link	Shared interests include societal standards, politics, and power, as well as security considerations. The level of internet censorship differs from nation to nation. While some democratic nations moderately restrict access to the Internet, others go so far as to restrict residents' ability to access news and other forms of information. Additionally, internet filtering happens in response to or ahead of riots, protests, and elections.	Legal control over what people can access on the internet is known as censorship .Blocking Internet Protocol (IP) addresses It is not possible to access a certain IP address. Websites on the same server will be prohibited if the target website is located on a shared hosting server. This impacts many protocols, including FTP, POP, and HTTP. Websites are the usual target of circumvention techniques, however proxies can be congested or restricted, and some websites, like Google, have been given extra IP addresses to get around the block.
How Internet Censorship Works https://computer.howstuffworks.com/internet-censorship.htm	While some censorship opponents contend that parental monitoring is the greatest approach to keep children safe online, many parents point out that this is challenging, and many, if not all of them, resort to single-source hardware solutions as a solution. Users can acquire Web filtering tools such as Cybersitter or Net Nanny to prevent access to unwanted websites. Parents can choose from a range of features in these programs to restrict the websites that their kids can visit. These settings instruct the software on which fitters to activate. For instance, CYBERsitter offers 35 filter categories, such as social networking sites and pornography.	To deliver users relevant search terms, the majority of search engines self-censor their search engine results pages (SERPs). This is required because some webmasters attempt to manipulate search engines so that their web pages appear highly in search results. Every search engine result page would contain irrelevant results if search engines didn't filter and analyze these pages. An online page known as a proxy site enables you to access the internet without utilizing your IP address. You go to the website, which opens a text field where you may enter the URL of any restricted website you'd like to access. After retrieving the data, the proxy website shows it. Only the fact that you accessed the proxy site—not the websites you've visited—is visible to outsiders.

• "Free Speech Or Hate Speech: When Does Online Hate Speech Become A Real Threat?" (audio article): link	Before committing a crime, online users frequently make posts about hate speech.It is the victims' perception that not enough is being done to stop or prevent these remarks and actions from occurring. Certain hate speech has been connected to terrorism, such as the bomber who delivered explosives or the mass shooter who shared hateful content online. Some people think social media is not to blame as it does not cause people's deaths directly. Moreover, censorship might increase security.	The first amendment and social media equals constitutional right to free expression
• Internet Censorship Explained" (video): link	The protection of privacy and anonymity guarantees that censorship resistance system users cannot be identified.	The primary elements of communication are the subject matter (the information) and the parties involved (the user and publisher). They may potentially send TCP reset packets to both parties or take further action and send drop packets to censor and disrupt communication if they detect a damaging or hateful phrase. A censor finds it challenging to keep track of the vast amounts of information available on social media sites like Facebook and Twitter.

Name(s) sharena sharif   Period 5, 6   Date 11/13/23

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
Fill in the table below with your Impacted Groups. You may optionally add new groups or split one of the ones assigned into smaller subgroups if it will help better explain who's involved in the dilemma.

Impacted Group and Description	Interests, Benefits, and Harms
Group 1: Everyday internet user anyone browsing, those who access the Internet whether at home, at work or from anywhere else; whether for private or professional purposes; regardless of the device or type of connection used,	- create a safer online environment by shielding consumers from scams, harmful content, and other online risks. - censorship can make the internet a more pleasant place by preventing the spread of

approximately everyday or very often.	offensive, violent, or radical content. - help create a more polite online society by preventing the spread of offensive and dangerous content. - restrict access to a variety of viewpoints, making it more difficult for users to investigate various concepts and viewpoints. - censorship has the potential to silence critics and opposing views, users may feel that their freedom to speak their thoughts is being violated. - restricting the availability of particular kinds of content and ideas, unduly restrictive policies may discourage creativity and innovation. - people who use VPNs or other tools to get around restrictions may end up with legal issues + other inconveniences.
Group 2: Intelligence Agencies government agency tasked with obtaining political or military intelligence, particularly for national security purposes	- limits the danger of radicalization and recruitment online and prevents the spread of sensitive information. - difficult for the government agencies to keep an eye on and obtain information from specific web platforms, which would complicate monitoring operations. - for intelligence organizations, striking a balance between censoring dangerous content and preserving access to vital intelligence is a difficult task. - the use of censorship techniques can help stop the spread of private information that can endanger national security. - internet filtering can play a significant role in halting extremist groups' online activity and averting radicalization. - cybercrime, fraud, and illicit commerce are just a few of the online illegal behaviors that may be monitored and reduced with the use of censorship. - intelligence agencies may be able to better manage the narrative and information flow by limiting particular sorts of content. - increasing worries about civil rights and privacy, which could spark criticism from the public and legal issues. - may affect reliable information sources, impeding the collection of intelligence from non-threatening sources. - cross-border censorship implementation can be difficult, requiring collaboration from other countries and perhaps strained diplomatic ties.
Group 3: Political Activists a person who actively supports social or political change and engages in actions like demonstrations in the community	- preventing the spread of false information and shielding them from specific threats. - restricting their capacity to organize movements, voice opposition, and access different viewpoints, which can affect their right to free speech and their capacity to rally support.

	- protected by censorship from targeted assaults, threats, and abuse they receive online. - restricting distribution of extreme beliefs that might endanger political activists and the general public can be achieved by censoring extremist material. - prevent spread of information during political events / movements that might inspire violence or cause chaos in the community.

Technical Background
Explain the technical background necessary to understand the problem. Include:

- *Background on layers / protocols / principles of the Internet necessary to understand the dilemma*
- *Use the concept bank on the first page to help brainstorm ideas to include. A strong description will reference several of these concepts*
- *Make sure your descriptions are approachable for your candidate, who does not have as strong of a background in the way the Internet works*
- *This can be completed in bullets*

-The primary components of communication are the subject matter being discussed (the information) and the person (the user) speaking with the publisher.
-They may send a TCP reset packet to both parties or take other action, such as dropping packets, in order to obstruct and filter communication if they detect a damaging or nasty phrase.
-A censor finds it challenging to keep up with the massive amounts of data from social media sites like Facebook and Twitter. Everything is always changing.
-The government and parents are not the only ones that use internet filtering. Numerous software applications are available for consumers that have the ability to restrict or prevent access to particular websites.(online filter)
-Filtering and blocking are frequently inaccessible to users of the blocking software and are based on either more dynamically generated blacklists or relatively static blacklists.
-To give consumers relevant search results pages (SERPs), the majority of search engines self-censor their SERPs. Tass is required sometimes because some webmasters attempt to deceive users into believing that websites have high search engine ranks. Every search engine result page would be flooded with irrelevant results if the search engines didn't filter and remove these pages.

Recommended Policy Solution
Give a recommendation for what policy or solution your candidate should advocate for. Your solution could be a law that should be passed or repealed, a government policy, or a technological solution your candidate should promote.

Recommended Policy: *In at most two sentences summarize the solution / action your candidate should support*
Before anything is published, internet service providers must work with content owners and government representatives to monitor, restrict, and remove any dangerous content that could endanger national security or encourage unlawful activity.

Pros / Who Benefits	Cons / Who is Harmed?
● *National Security Agencies: Benefit from the prevention of the transmission of sensitive information and the decrease of cyber threats.* ● *Governments: Acquire resources to uphold public safety and shield citizens from possible danger.* ● *Law enforcement: Made it easier to look into and stop illegal activity that takes place online.* ● *Public: Take advantage of a safer online space*	● *Advocates for freedom of speech: Worries about possible restrictions on voicing disagreement and differing viewpoints.* ● *Individual Privacy: Dangers of greater government data collecting and surveillance.* ● *Information Access and Innovation: Possible restrictions on information availability and suppression of online creativity.* ● *Political activists: The difficulties of organizing*

with less exposure to offensive material.	*movements and voicing disapproval without excessive constraints*

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