A Cross-Cultural Analysis of Internet Governance Between the U.S. and China

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

George Noonan
Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____
George Noonan

Approved _____ Date _____
Tsai-Hsuan Ku, Department of Engineering and Society

Introduction

It is all too common today to read or hear in western media about the rise of authoritarian China and its Orwellian censorship apparatus. This view, although entertaining, is inaccurate and full of western bias and ignorance of Chinese culture. It does not take into account the social and political factors that shape the Chinese concept of the internet, which is necessary to overcome the simplistic western view of an evil dictatorship. Furthermore, it is becoming more important to develop a more accurate understanding of China as continues to grow into one of the most powerful countries on the planet – technologically and economically. Recent geopolitical tensions are a sign of this, with the United States and China locked in a competition for the future of global leadership. One area the competition is extreme is the internet, which represents a crucial domain for both countries and an opportunity to define the future of telecommunication standards. With the rollout of fifth generation telecommunication networks, both countries are facilitating a bifurcation of the internet – each part a reflection of the cultural and political values of that country. In addition, the technology is making the internet even more essential in everyday life as more and more devices are connected. It is thus imperative to research the historical, social and political factors behind the U.S. and China's divergent internet implementations and provide a cultural analysis between the systems of the two superpowers.

Literature Review

History:

The internet officially started in 1962 when MIT professor J.C.R. Licklider conceptualized messages being sent over a network – similar to the internet that exists today.

This event marked the birth of the internet, and it eventually inspired several researchers at Defense Advanced Research Projects Agency (DARPA) to develop the idea a network of computers, which they named "ARPANET". A breakthrough occurred in using packets to send information in the network instead of a traditional circuit, and the first network node was built at UCLA. Soon after, Stanford and several other universities established their own nodes on the network and successfully sent the first message (Leiner, 2009). By the 1980s, the internet in America was starting to become commercialized as more uses of the technology were introduced. Not only were individual companies commercializing the internet to sell their products, but new private network service providers and private ISPs were commercializing the actual service and infrastructure (Leiner, 2009). This is a stark contrast to the development of the internet in China, which has maintained a state managed, centralized approach to development that is described in a later section. The U.S. took the opposite approach of a free and open internet though beginning in the 1980s. Even though the internet was created by the government as a military research project, the subsequent development and innovation of the technology was dominated by the public and commercial actors. In other words, the commercial actors – corporations, ISPs, consumer interests – dominated the development of the internet in the country while the government and civilian actors played a smaller, but still important role. Even though this strategy was successful in making the U.S. a world leader in internet technologies today, China took a more centralized, state-led approach that has positioned the country as an equally capable competitor for deciding the future of the internet.

The Chinese internet we know today is a result of rapid state investment and growth in an industry that otherwise had a slow start relative to the global community. One contributor to the slow start is the country's history of going through periods of isolation – such as when Mao

Zedong was ruler. That is not to say China has always taken this approach, as there are also several periods of the country opening up to the world, such as during the rule of Deng Xiaoping. This period began around the late 1970s, with the Chinese Communist Party opening up the economy to reforms and shifting its focus to science and technology. According to a publication in the Association for Computing Machinery, the Chinese government views the internet as an essential tool for achieving economic growth. However, its policies incorporate a balance between promoting economic incentives for developing the internet and maintaining power and social stability among its citizens (Yang, 2012). During the period of opening up and several decades after the invention of the internet in the U.S., a fully functional version of the internet was released in China in 1995 for public use. Not only this, but state investment also increased significantly. Contrast this with the U.S., where the government dominated the development initially, but ultimately capitalist actors shaped the internet we know and use today. The investment made by the Chinese Communist Party was no small amount either. From 1997 to 2009, the government spent over six hundred billion dollars investing in internet infrastructure and in 2008 surpassed the U.S. to become the country with the most internet users (Barboza, 2008). Such rapid development is impressive, and it is a result of the government's dominant role in Chinese society and its early prioritization of the internet as a source of economic output.

Internet Use

In the U.S., it is easy to assume that the internet is an open, unfiltered tool for the liberation of ideas and access to uncensored content. However, similar to the western view of China being a repressive regime, it is too simplistic of a representation of internet use in the U.S. While it is true that American netizens have nearly unfettered access to content online – a stark

contrast to the internet in China - the government is still a very powerful actor in the system. Consider PRISM, a government created program that collects private user data from the world's most popular services like Google, Facebook, Outlook, Apple and more (Sottek et al., 2013). Moreover, the program is owned and operated by the government's national security groups, giving it enormous power over the internet and the lives of American citizens. Documents leaked around the time of Edward Snowden describe the government being able to obtain a particular person's data even without a warrant. Instead, special secretive courts called FISA courts approve ways of collecting data and not the actual instances of data being collected (Greenwald et al., 2017). This should be a red flag to anyone with a basic interest in privacy: a right held so dearly by Americans that it is protected under the fourth amendment. One would think this right extends to the internet, and perhaps it is simply that the technology's development has outpaced regulation. Nevertheless, the FISA courts and pervasive surveillance still play an authoritative role in shaping internet usage in the west. This is a clear contradiction to the commonly held idea of a western internet dominated by liberal ideas and unfettered access, and it shows that the government acts as a powerful actor despite the dominant role companies have played in shaping the internet of the western world.

Similar to how internet in the United States is characterized by a simplistic ideological view, it is all too common to hear about the strict censorship controls under the Great Firewall of China (GFC) as tools of an oppressive, authoritarian regime. This perspective is incomplete, and we must reject it in favor of a more holistic view that views the internet through the lens of Chinese culture and society. At AngelHack – the world's largest and most diverse global developer ecosystem – director Matt Right supports this when he asserts that it is normal in Chinese culture to accept the absolute authority of the Chinese Communist Party (CCP). For

people who grow up in China, they spend their whole lives living with the fact that the government has complete access to anything about them (Jacobs, 2018). In a way, Chinese citizens view the internet as simply another extension of their lives, and they thus do not have a problem with the lack of privacy over the internet. To them, it is no different than in the real world: there is no privacy either way. Associate professor at Cheung Kong Graduate School of Business Dr. Zhang Weining seems to agree, claiming that Chinese people value other things more than privacy. According to him, building wealth and convenience are the top reasons why Chinese users have no issues sacrificing privacy (Jacobs, 2018). With these insights into the lack of cultural value placed on privacy in China, it is clear that the simplistic view cannot be accurate. That is, the view that its citizens are being repressed is incorrect because according to Zhang, people are actually more worried about achieving their goals than their privacy. Compare this with the U.S., where privacy is considered a fundamental right, yet is still being exploited through PRISM and other surveillance technologies. In light of this, it cannot be justified to characterize the internet in China as an Orwellian tool: Chinese culture simply does not place as much value on privacy as in the west. Moreover, the strict internet monitoring in China is a reflection of the lack of emphasis on privacy, and it can hardly be representative of an internet designed to repress its people.

STS Framework: Political-Social-Cultural Roots of Engineering Ethics

We can better understand the issue of information governance by looking through the lens of political and economic competition between the United States and China. Both countries pursue competition with each other through their cultural, social and political roots, and

information governance and censorship in the two countries are heavily influenced by these factors.

Beginning with the U.S., individuality and natural "rights" are core issues of data governance and censorship policies, and companies that do not share these values have been under criticism lately. In the U.S., all information on the internet is protected by the First Amendment, preventing censorship on the local, state and federal level. A clear reflection of the "right to free speech" that Americans cherish, this law allows users to say whatever they wish online. However, it is important to note that the U.S. government has the ability to forcefully shut down servers, which was the case for infamous torrent website The Pirate Bay and WikiLeaks, thereby having the ability to restrict information online to a degree. Although this conflicts with the idea of free speech and individuality to host whatever content one wishes, the First Amendment importantly protects information critical of the government – especially information that would not be allowed to be online in China.

In addition to the values of free speech and individuality determining the structure and governance of information in the U.S., the ideas of limited government also apply. Since declaring independence in 1776, the American people have long cherished limited government as the best way to govern their daily lives. This value extends to the internet, where content regulation is mostly done at the private level and is not mandated by the government. This is a result of both limited government and the belief that private interests take priority over the public benefit.

Unlike in the U.S., Chinese culture values the public benefit over private interests, which has been a key factor in the development of the "Great Firewall" censorship apparatus. Whether or not you believe the Chinese Communist Party is serving the interests of their people, you

cannot ignore the impact that their collective culture has over information governance in the country. Censorship is used as a means to promote unity among the Chinese people because if everyone only has the access to the same information, then the cohesiveness of its citizens will be enhanced. From a western perspective, this "forced" collectivism is a way for the CCP to tighten its control over its citizens; from a Chinese perspective, it is implementation of the internet that reflects Chinese collectivism and placing the public needs above their own individual ones.

Besides being a reflection of the cultural values placed in collectivism and putting the public benefit over private interests, government information censorship is also an incorporation of individual responsibility and sacrificing one's needs. These cultural and societal values are paramount to the development of the Great Firewall in China because the censorship apparatus is an implementation of the internet that includes these ideas: an internet with Chinese characteristics.

STS Framework: Surveillance Capitalism and Cyberspace Sovereignty

Surveillance capitalism poses an enormous risk to the United States because they threaten the individuality and "rights" so cherished in American society. The most prominent threats come from tech giants like Google, Facebook and Twitter – particularly Facebook – because these companies rely on human capital to collect data, predict and control their user's behavior, and ultimately to satisfy their business models. In addition, each of these companies provides the government with surveillance access through their platforms, virtually eliminating the right to privacy and the Fourth Amendment that protects against unreasonable searches. While

surveillance capitalism poses a threat to the openness of information in the U.S., China has recognized another problem that is equally as important: cyberspace sovereignty.

When it comes to cyberspace sovereignty, China is ahead of the game. Not only did they recognize the importance of protecting one's internet from other sovereign – mostly hostile - nations, but they quickly prioritized it as an issue of importance as high as that of traditional military branches. As explained in the previous section, collectiveness is a value that propagates through eh Chinese implementation of their internet. This collectiveness and sacrifice of the individual is the result of their value of placing society before ones needs, which ultimately comes back to the CCP. Unlike in the U.S., where the "openness" and individual are being challenged by all too powerful tech companies and the corporate-government partnership in surveilling the internet, the CCP recognized this as a threat and sought complete control over information governance in the country. While this may enhance the collective societal values in the country, it also might do the opposite: concentrate the power too much in a few government leaders instead of serving the public good.

Data Analysis

Since most American citizens do not even know about PRISM, it is imperative to illustrate the massive scale at which internet in the United States is being monitored. According to an article published in Computer Weekly and Ashford (2013), the data collected through PRISM amounts to a "treasure trove" and the full extent to which it operates is known by few, if any. Interestingly though, the author also points out that the media has likely exaggerated the amount of data collected by the government's algorithm – although it is impossible to say for sure (Ashford, 2013). According to an article published in the Guardian, PRISM started

collecting data in 2007 from all the major U.S. internet companies: Microsoft, Yahoo, Google, Facebook, Apple – just to name a few (Sottek, 2013). It achieves this through direct access to the company's servers, which is not only a gross privacy violation, but it also positions the government as the dominant actor in the western internet. Since virtually all of the major corporations are being monitored, there is little the average internet user can do to protect their data from the government. This is further supported by the corporations categorically denying knowledge of the technology to the media (Greenwald, 2017). This a concern for any privacy advocates, and it certainly runs counter to the myth that internet in the United States is an unfettered place for the liberalization of ideas. To further illustrate the extent of surveillance, the number of obtained communications in 2012 over Skype increased by 248%, Facebook by 131% and Google by 63% (Greenwald et al., 2017). This is just one year's worth of surveillance increase: envision how much it has increased in the past nine years. Still though, Americans do not seem to be united against the mass surveillance. Former US government CIO and executive director of information security certification organization Hord Tipton argues that since Edward Snowden revealed PRSIM to the world, western society has been polarized on the issue (Ashford, 2013). Some think that millions of people's privacy has been violated, while others see his actions as putting privacy at even greater risk. Managing Director of Jirasek Consulting Services Vladimir Jirasek seems to agree with the latter view, arguing that the NSA, FBI and CIA – with over 100,000 authorized users - is highly susceptible to attacks because of its vast access to data of millions of people around the world (Ashford, 2013). Regardless of which view one takes, it is evident that internet surveillance is ubiquitous in western society and that the American values of freedom and privacy are not reflected in the internet today.

Similar to the United States, China also conducts mass surveillance on its 800 million netizens. However, surveillance is not the only tool available to the Chinese Communist Party as they also have absolute authority over regulating content. Censorship is common in the country, and according to human rights group Freedom House, China scores a mere 10/100 score for online freedom and has one of the least free internets on the planet. The report analyzed factors such as obstacles to internet access, limits on content and violation of user rights which scored 8/25, 2/35 and 0/40 respectively (Chan, 2015). Clearly, the government in China has total control over the infrastructure and content in the country's internet. That being said, it does not mean the absolute authority is a reflection of the western view of a repressive dictatorship. One recent example of the government's handling of COVID-19 disinformation shows that the less free Chinese internet was actually more effective.

Fake news has been a prominent issue in recent years, and the way the U.S. and China each handled the issue could not be more different. To regulate content in China, there is a group of media and internet companies called the Beijing District Joint Anti Online Rumor Platform (BJARP) that regulates content online. Interestingly, its functions are to "disseminate valid and correct information" and to "refute rumors" (Chin, 2019). These functions are broadly defined, and it would thus be easy for the government to label any disseminating information as a rumor or incorrect. However, they are also very effective at combatting real fake information online. Consider that the Chinese government owns all the ISPs in the country and is the IP address authority. In addition, there are several root DNS servers hosted in China. These tools, in combination with BJARP are highly effective at regulating content over the internet. When COVID-19 occurred in the country, the government's absolute control over the internet infrastructure and services like WeChat allowed it to quickly adapt its mass surveillance system

to record health data. All of the data was fed through a government-controlled algorithm that helped quarantine infected people and slow the spread of the virus (Chaturvedi et al., 2020). In this case, the government's absolute control over the internet actually made it more effective at helping its citizens control the spread of the virus. This represents yet another contradiction to the simplistic view that the CCP represses its citizens through the internet. It was actually helping them in the most efficient way.

Compared to China, the U.S. response over the internet to COVID-19 was chaotic and inefficient. When the pandemic was spreading in the country, individuals on social media, public leaders, and the media spread misinformation about the pandemic and basic facts about the severity of the situation (Bagherpour, 2020). Even the President of the United States helped spread false information about Hydroxychloroquine being an effective means to stop COVID. The government may have a lot of power to spy on internet traffic, but it does not have the authority to censor false information like the Chinese government. This fact makes combating disinformation in the U.S. very difficult, and it has left social media companies filling the void and instituting their own disinformation policies. However, there is no cohesion or consensus on how to regulate fake content – even to this day – which has made the country's response to disinformation disorganized and inefficient. That being said, there has been a lot of debate as to how to approach the problem. For example, an article in the Scientific American suggests having influential people on social media work with reputable doctors and health specialists. In addition, it mentions the collaboration between corporate and government actors to combat disinformation on social media platforms (Bagherpour, 2020). Perhaps this would be an effective way to approach the issue, although it still remains to be implemented and government regulation still lags behind technological innovation in the country. While many see the openness and liberation

of the internet in the U.S. as a positive trait, pervasive disinformation has shown that it has its drawbacks compared to the Great Firewall of China and is not always the best solution in serving the people.

Conclusion

While it is easy to believe the basic idea that the U.S. and China are interlocked in an ideological competition for the future of the internet, it is crucial to understand each countries vision through the context of history, culture and politics. Just as it has been shown, the two countries are more similar in their versions of the internet than one might think. Both systems are affected by strong government actors, whether through PRISM or the Great Firewall of China. Moreover, Chinese culture places a much smaller emphasis on privacy and the stringent internet controls are a reflection of this value: citizens simply do not care they are being monitored. Americans, on the other hand, have long held privacy as an essential value by incorporating it into the constitution. They too, however, are being closely watched and in most cases, without any indication whatsoever. Thus, the two systems are not all that different after all, except in one country the internet surveillance is generally accepted while in the other it is simply not common knowledge. Lastly, it has been shown that the strict internet controls in China were more effective at combatting disinformation than in the U.S. This is an important example that contradicts the simplistic ideological view that the open, free internet is “better”, and it shows that the Chinese system can be more effective in some cases. Nevertheless, it is important to keep these points in mind when comparing the internet in China and the U.S. After all, whichever country wins the ongoing technological competition will define the future of the internet.

References

Ashford, W. (2013, October). *After Prism Revelations There is Nowhere to Hide*. Computer Weekly.

Bagherpour, A. (2020, October 11). *COVID Misinformation Is Killing People*. Scientific American. https://www.scientificamerican.com/article/covid-misinformation-is-killing-people1/.

Barboza, D. (2008, July 26). *China Surpasses U.S. in Number of Internet Users*. The New York Times. https://www.nytimes.com/2008/07/26/business/worldbusiness/26internet.html

Chan, E. (2015, November 5). *The Great Firewall of China*. Bloomberg. https://www.bloomberg.com/quicktake/great-firewall-of-china

Chaturvedi-, A., By, -, Editor, A. C. F. A., Chaturvedi, A., & Editor, F. A. (2020, May 11). *The China way: Use of technology to combat Covid-19*. Geospatial World. https://www.geospatialworld.net/article/the-sino-approach-use-of-technology-to-combat-covid-19/.

Chin, Yik Chan. (January 5, 2019). *Internet Governance in China: The Network Governance Approach*. https://ssrn.com/abstract=3310921 or http://dx.doi.org/10.2139/ssrn.3310921

Greenwald, G., & MacAskill, E. (2017, December 29). *NSA Prism program taps in to user data of Apple, Google and others*. The Guardian. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Jacobs, H. (2018, June 26). *Chinese people don't care about privacy on the internet - here's why, according to a top professor in China*. Business Insider. https://www.businessinsider.com/why-china-chinese-people-dont-care-about-privacy-2018-6.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2009). *A brief history of the internet.* ACM SIGCOMM Computer Communication Review, 39(5), 22–31. https://doi.org/10.1145/1629607.1629613

Liao, S. (2018, February 1). How WeChat came to rule China. https://www.theverge.com/2018/2/1/16721230/wechat-china-app-mini-programs-messaging-electronic-id-system.

Sottek, T. C., & Kopfstein, J. (2013, July 17). *Everything you need to know about PRISM*. The Verge. https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

Yang, G. (2012). *A Chinese Internet? History, practice, and globalization.* Chinese Journal of Communication, 5(1), 49-54. doi: 10.1080/17544750.2011.647744