Methods for Increasing Data Control and Bypassing Censorship Online

Cross-Cultural Analysis of Information Governance in the United States and China

A Thesis Prospectus Submitted to the

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

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

Technical Project Team Members:
George Noonan

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 _____

Approved Aaron Bloomfield Date _____

Aaron Bloomfield, Department of Computer Science

Approved _____ Date _____

Tsai-Hsuan Ku, Department of Engineering and Society

Introduction

With the number of devices connected to the internet surpassing twenty-two billion, data has become a ubiquitous part of our daily lives. We are all part of the data industry to some degree. This has heightened the importance of data control and how information is being governed online. As my STS prospectus explores, internet companies in the U.S. and the government in China are the main actors involved in the system. What about the everyday netizens? My technical topic will explore actionable ways these users can exert their power in the information governance system by taking control of their data and bypassing government censorship.

Technical Topic

My technical project will explore the practical ways in which an internet user can increase their control over their data and bypass government censorship. I plan to accomplish this through exploring social media privacy settings, data encryption, network traffic encryption and password keychain tools. Specifically, I will investigate ways in which users can adjust settings on popular websites Twitter and Facebook to increase their control over their data. I will also explore whether changing settings will reduce the power that social media companies have over our data. Although these two topics are similar, one does not necessarily imply the other.

Besides social media settings, I will also explore ways a user can encrypt their data, whether it be files on their computer, phone or on the cloud. Encryption can ensure a user's data remains confidential, available and unmodified. Furthermore, it can be used to ensure privacy over internet companies and the government. One popular tool I will explore is an open sourced program called AESCrypt. It allows users to encrypt files with 256-bit AES encryption.

In addition to researching ways a user can encrypt data and individual files, I will also evaluate the effectiveness of virtual private networks (VPN) and encrypted network traffic. There is a common misconception that VPNs make your internet traffic private. However, this is not the case at all. Using an unencrypted VPN will make all of your data available to the company who provides the VPN. However, using an encrypted VPN can make it very difficult for others to access a user's data. I will explore the ways this can be accomplished, as well as how encrypted virtual private networks can be used to bypass government censorship. Having first-hand experience doing this in China, I know that it is an effective means to access the open internet.

Finally, I will examine password keychain tools, such as iCloud Keychain, and whether it gives a user more or less control over their login credentials. Since the keychain can store highly sensitive information such as your address, credit card numbers and health data, it is imperative that this data be secure.

STS Prospectus

Introduction

I have lived in China for a year and studied abroad during the 2019 protests in Hong Kong, so this topic is particularly important to me. While I was there, police were censoring content on WhatsApp and WeChat to identify and dox protestors. I also witnessed censorship in person as anti-China posters and flyers were frequently removed from walls at my school and neighborhood. That being said, China is not the only country using censorship, and it should be no surprise that many countries do it to some degree.

Research Questions:

What social, economic, and political factors shape China and the United States' strategies towards information governance?

How do power dynamics between different stakeholders contribute to the meaning and implementation of information governance in the U.S. and China?

How is information control achieved using telecommunications in the U.S. and China? Are there other methods?

Literature Review:

There is a simplistic view common in western media that China has an authoritarian government that represses its citizens through the Great Firewall and strict data control laws. However, this view does not hold for cases such as the 2007 chemical plant incident in Xiamen, China. Upon discovering the toxic plant would significantly pollute local neighborhoods,

Xiamen citizens expressed their anger online. These messages were quickly censored by the government – aligning with the simplistic view of a repressive government - but the citizens were so angry they continued to protest online and arranged a real protest with over 20,000 people. The government eventually scrapped plans for the chemical plant (Liu Jun, et al.). If the Chinese Communist Party (CCP) was the totalitarian government the west sees it as, then why would it listen to its citizens? Questions like this can only be explained by evaluating information governance in the context of culture and society because evaluating the Chinese system from a western perspective is clearly inadequate.

Just as with China, information governance in the United States must also be analyzed as a sociotechnical system to fully grasp the meaning and purpose of censorship in the country. Democracy, freedom of speech, and capitalism are ingredients in this system, and different stakeholders in the U.S. prioritize each differently. Internet companies, for example, currently have more incentive to maximize profit than to protect freedom of speech. The Communication Decency Act (*47 U.S. Code § 230*), protects these companies from the content their users post, and recent events indicate that many internet companies care most about profit. One notable example is Facebooks recent refusal to stop displaying political ads. It cannot be ignored that Facebook is a publicly traded company with the sole purpose of maximizing shareholder return, and these advertisements provide extra revenue for Facebook that other internet companies sacrificed to reduce hate speech. Although censorship is not a mission of most American social media companies, many employ algorithms and staff to remove hateful content and prevent the spread of misinformation. Twitter has a list of rules that define the information allowed and not allowed on the platform. Interestingly, many of the rules are vague such as the platform's ban on "manipulated media that is likely to cause harm" (Twitter). What constitutes "likely" is very

subjective, and such vagueness enables political bias. This is one of the many complexities that comes with information governance in the U.S, and the broader impact of the technical-political relationship is that internet companies currently hold enormous influence and power over the meaning of censorship and regulation of free speech in the U.S. While the federal government has traditionally been the driving actor in regulating traditional media companies, it has allowed large companies to independently decide – according to the Communication Decency Act - their information censorship policies and thereby invite political bias onto their platforms (*47 U.S. Code § 230)*.

This is a critical issue in today's world because billions of users around the world rely on the internet and cloud-based service providers to handle their data (N. Al-Mhabis et al., 2005). With so much data, everyone is a part of the information governance system. An STS investigation into this topic would explore the cultural and ethical considerations of information censorship. What is censorship? Can it be good? What differentiates good censorship from bad? Is there one form of information control that would work for one country and culture but not another? These are all open-ended questions with no clear answer. This is a great topic to explore in the context of society because the recent geopolitical rift between China and the United States and their conflicting world views have prevented a consensus on how information governance should be implemented.

STS Framework and Method:

<u>Large Technical System:</u>

Hughes' perspective of a Large Technical System (LTS) can be applied by first identifying the key components of the system. The system builders include governments, private companies, academic institutions, the military and entrepreneurs. Although these system builders are consistent across different societies, the balance of power between each builder is different in the U.S. and China. In the U.S., social media and traditional media companies play a more active role in censorship and information governance than the government and military (Shah et al., 2005). However, in China, the government and military have the ultimate authority in restricting content online and private companies have less power to censor information in the technical system.

In addition to identifying the system builders, we can also apply Hughes' perspective by discussing the role technological momentum has played in information censorship. The biggest factors contributing to technological momentum have been the invention of the internet and the introduction of IoT. Since its advent, the internet has created economic opportunities across government, military, commerce and entertainment. These economic opportunities are enough on their own to provide momentum for information governance within the technical system, and they are increasing even more as IoT becomes ubiquitous in modern society. As governments, private companies and academic institutions rely more heavily on the internet and online information, the momentum to define and adopt their own information governance policies will only increase. In addition, there has been a large technological rift between China and the U.S. in the past years. Considering both countries are at the forefront of information technology, it is only natural that the geopolitical rift accelerates the divergence between how information governance occurs within the two countries (Levite et al., 2019). As a result, there has recently been increased importance for information governance in both countries, particularly information

traveling internationally (Schia et al., 2018). The final component of information governance that we can apply Hughes' perspective to is to describe the reverse salients in the system. In the U.S., the deep desire for free speech and freedom has prevented the government from regulating information governance and left social media companies to fill the void themselves – per the Communication Decency Act (Allyn, 2020). However, there is still no consensus on information governance in the U.S., and the lack of agreement has acted as a reverse salient in the technical system. The Stop Hate for Profit campaign – supported by respected companies such as Procter & Gamble and The North Face - has recently demanded Facebook censor hate speech on its platform (Atkinson, 2020), illustrating the divide among the system builders on how information governance should be accomplished online. Compared to the U.S., there is a much stronger consensus about information governance in China because the government acts as the ultimate arbiter. However, the heavy-handed information censorship approach in China could also be viewed as a reverse salient in the system, because even though there is consensus, the chances are higher that it's a consensus for a subpar solution.

SCOT Framework:

In order to apply Pinch & Bijker's SCOT framework to the sociotechnical system of information governance, first identify the relevant social groups. Information governance is a broad topic, but the focus can be narrowed to the U.S. and Chinese governments, social media companies, telecommunications companies, algorithm developers, academic institutions, and regular internet surfing "netizens" from both countries.

Beginning with the U.S., social media companies and algorithm developers have the most power and influence over information censorship policies in the country. Since social media companies have yet to be regulated by the U.S. government, many such companies practice self-censorship on their platforms and rely on their developers to build the highly sophisticated censorship algorithms. In addition, with millions of users and valuations larger than many countries' entire GDP, social media companies enjoy an enormous degree of power and independence over their information governance policies.

Unlike in the U.S., the power dynamics in the information governance system in China are dominated by the government. In China, the government has supreme control over information through the Great Firewall and National Intelligence Law. These mechanisms make the Chinese Communist Party the ultimate arbiter in any information governance policy and the most powerful actor among the relevant social groups. Not only this, but the government regularly censors its netizens who post anti-CCP content or anything that would hurt the governments image. Clearly the government holds the reigns over information in China, although not always as a repressive dictator as commonly believed. One counter example was the aforementioned chemical plant in Xiamen. Although the government knew its citizens were successfully bypassing the ban, they ultimately listened to the citizens and gave them what they demanded.

Now that the relevant social groups in our information governance sociotechnical system have been identified, we can start revealing the interpretational flexibility. Beginning with the U.S., consider what a "good design" of information governance would look like for each relevant social group. For the government and netizens, an idea solution could be one that perfectly

follows the constitution and law regarding other information (books, newspapers, etc.); the internet should not be regulated any differently. Social media companies, on the other hand, have the main objective of maximizing profit, so their information governance system will be one which enriches the company the most in both the short and long-term. This can carry political weight and intentions, such as Facebook refusing to block political misinformation on its platform: by refusing to limit ads, the company is fulfilling its primary objective of profit maximization. Academic institutions in the U.S. support a free, open internet for the good of education and society, so the ideal information governance system will be a lack thereof.

Unlike in the U.S., the interpretational flexibility of information governance is dominated by the government and it is difficult to tell what an ideal design would look like to any actor outside the government. Since the government is the most powerful relevant social group in China, we can compare its understanding and ascribed meanings on information governance to that of the social groups in the U.S. The Chinese Communist Party relies on information governance as a means to consolidate power and suppress opposing viewpoints online. However, as mentioned previously, this is a simplistic view of Chinese society and it is a common opinion among westerns. It ignores the fact that Chinese culture and society place high emphasis on collectivism, and we can view the absolute control over information in the country as a means of promoting cultural collectivism. The government is no evil dictator. Instead, it relies on information censorship to control public opinion and promote collectivism and trust between Chinese society and government.

The last way the SCOT model can be applied to information governance is by discussing the potential for closure in the ongoing tech conflict between the U.S. and China. The two

countries are involved in what seems to be a cold war, and it does not seem likely that the conflict will be resolved soon. It is unclear whether one system will win over the other, or if an entirely new system of information governance will arise from the conflict. Regardless of the outcome, China and the U.S. must work together to solve their ideological differences and agree on a method of information governance.

Methods for Data Collection:

For this investigation, both primary and secondary sources will be used to gain a deeper understanding of the cross-cultural implications of information governance in the U.S. and China. For primary sources, news articles and policy documents from companies and the government in both countries will be used to compare the politics of information governance in both countries. This comparison will be strengthened by secondary sources – primarily books and academic papers - which will provide a deeper perspective on public perception and the cultural and societal implications of censorship. Finally, quantitative data on the mechanisms through which information is censored online will be incorporated to supplement the cultural and societal comparison with a technical perspective.

Timeline:

My research plan going forward is to find more sources comparing the politics of the Chinese and American internet governance approaches. The more there are, the stronger evidence there is to provide a cross-cultural analysis.

Conclusion:

While the STS prospectus analyzes and compares the socio-technical systems of information governance in the U.S. and China, the ultimate goal is to use the STS project prospectus to explore how users can become informed on their data and how it is being handled. Furthermore, my prospectus is about a very relevant topic in today's world, and its goal is to provide a more complete picture than the simplistic view of authoritarian China versus the democratic United States.

Bibliography:

47 U.S. Code § 230 - Protection for private blocking and screening of offensive material. (2018). Www.Law.Cornell.Edu/Uscode/Text/47/230. https://www.law.cornell.edu/uscode/text/47/230

Allyn, B. (2020, May 30). *As Trump Targets Twitter's Legal Shield, Experts Have A Warning*. Https://Www.Npr.Org/2020/05/30/865813960/as-Trump-Targets-Twitters-Legal-Shield-Experts-Have-a-Warning. https://www.npr.org/2020/05/30/865813960/as-trump-targets-twitters-legal-shield-experts-have-a-warning

Atkinson, C. (2020, June 22). *Facebook is facing its biggest backlash yet, as advertiser boycott gains momentum*. Https://Www.Nbcnews.Com/Business/Business-News/Facebook-Faces-Growing-Pressure-Advertisers-Do-More-Counteract-Hate-Speech-N1231786. https://www.nbcnews.com/business/business-news/facebook-faces-growing-pressure-advertisers-do-more-counteract-hate-speech-n1231786

Jun, L., & Hui, Z. (2010). Mobile Communication, Public Participation and e-Governance in China: A Case Study of Xiamen Anti-PX Demonstration. In *Proceedings of the 4th*

International Conference on Theory and Practice of Electronic Governance (pp. 327–332). Association for Computing Machinery.

Levite, A. E., & Jinghua, L. (2019, January 24). *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?* Https://Carnegieendowment.Org/2019/01/24/Chinese-American-Relations-in-Cyberspace-toward-Collaboration-or-Confrontation-Pub-78213. https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213

N. Al-Mhabis, & H. Cunningham (2017). Socio-political perspectives on surveillance and censorship: Implications for on-line privacy in the age of cloud computing. In *2017 Computing Conference* (pp. 208-213).

Pegoraro, R. (2020, July 28). *Here's Trump's Plan To Regulate Social Media*. Https://Www.Forbes.Com/Sites/Robpegoraro/2020/07/28/Heres-Trumps-Plan-to-Regulate-Social- Media/#4e28382062fa. https://www.forbes.com/sites/robpegoraro/2020/07/28/heres-trumps-plan-to-regulate-social-media/?sh=10c4639762fa

Schia, N. N., & Gjesvik, L. (2018, September 8). *The Chinese Cyber Sovereignty Concept (Part 1)*. Https://Theasiadialogue.Com/2018/09/07/the-Chinese-Cyber-Sovereignty-Concept-Part-1/. https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/

Shah, R., & Kesan, J. (2005). Governance Characteristics of Information Technology. In *Proceedings of the 2005 National Conference on Digital Government Research* (pp. 91–96). Digital Government Society of North America.

Twitter, Inc. (n.d.). *The Twitter Rules*. Https://Help.Twitter.Com/En/Rules-and-Policies/Twitter-Rules. https://help.twitter.com/en/rules-and-policies/twitter-rules