The Impact of Societal Views of Privacy on Data Collection Laws

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

Zane Belkhayat

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

Advisor

S. Travis Elliott, Department of Engineering and Society

STS Research Paper

Abstract

In a world already deeply entrenched in an “internet of things” there have been increasing repercussions for data collection on a scale and detail never before seen in history. Across the globe, consumer data is being tracked, catalogued, and even linked back to individuals at a greater and greater pace. This study aims to research how societal structures across the globe and views on data privacy impact the evolution of technology. Specifically, this research will delve into prior studies on individual countries such as the U.S and China. Aggregating the data, I hope to shed light on how prior cultural/societal structures impact the views, norms, legality and evolution of data collection technology in regards to the internet.

Introduction

During the current age of information, the world has faced a growing issue centered around data privacy. Between January and September of 2019 alone, there were over 7.9 billion data records exposed (Bekker, 2020). These issues have caused countries across the globe to begin adopting measures to protect consumers and examining current practices in regards to personal info. These measures vary from country to country together, as the concepts of acceptable privacy change with culture across the globe. This research paper aims to analyze how the evolution of societal artifacts and data collection technology influence each other through exploration of previous research. It will briefly cover the history of information privacy in the two countries (the United States and China) and analyze how their societal views impact the legislation and evolution of technology in regards to data privacy. These countries were chosen due to their differing approaches and backgrounds with regards to privacy and society, with one being from the east, having a communist background and one being from the west, having a capitalist background.

Social Construction of Technology

The framework of Social Construction of Technology (SCOT) posits that technology evolves in response to human action. In this way, society is the driving force behind the advancement of technology. Under the SCOT framework, there are three main points for analysis. These include “interpretative flexibility,” “relevant social groups,” and “stabilization.” Interpretative flexibility can be considered the driving force behind change in the SCOT framework. It assumes that there are multiple ways to interpret artifacts and each is equally as valid as another. However, these various interpretations give rise to problems of implementation. Considering the multiple ways to interpret, how does one synthesize the resulting ideas?

Relevant social groups are what give rise to the interpretative flexibility. Each social group invested in an artifact has a different background and intent when utilizing/interacting with artifacts. These backgrounds and intents give rise to the various ways in which social groups interpret said artifact. Finally, when the issue of interpretative flexibility begins to minimize that is seen as "stabilization" or closure. This comes in two main forms, known as rhetorical closure, and redefinition of the problem. Rhetorical closure occurs when social groups interpret the problem/artifact as being solved with need for alternative interpretation diminishing. This is often achieved through advertising. Redefinition of the problem occurs when the issues initially giving rise to interpretative flexibility are no longer focused on/redefined to be a different issue, which is solved by the artifact. Utilizing this framework, we can examine the link between societal views and the evolution of technology. Specifically, we can look to see how different cultural views in the U.S. and China give rise to social groups with different interpretations of privacy and how that influences the evolution of technology in both countries.

Background

Two countries which are heading in similar directions despite vastly different origins in the nature of privacy/data privacy are the U.S. and China. Analyzing them under the framework of SCOT leads to some interesting results. To begin, we will look at the early cultures of both the U.S. and China. The united states, being a fairly young nation does not have extensive history. Yet from its inception as colonies of the British Empire, the people of the United States have valued their privacy greatly. So much so, that one of the first few amendments, the fourth, begins alluding to it, with privacy against unreasonable search and seizure. The fourteenth amendment is also often cited as a right to privacy in its due process clause. However, nowhere in the constitution is there an explicit right to general privacy. As technology advanced regulation began to take shape in the

form of rules by the FTC, enforcing users' rights to determine what data is collected on them and how it may be used (Sharp, 2013).

On the other hand, China has a long and rich history, much of which was recently underpinned by Confucian ethics and morality. Confucianism came about during a period of much instability in Chinese society. In order to combat this, it placed order and governance above the rights of individuals. This is clearly reflected in the current Chinese culture and attitudes towards the government. The wellbeing and strength of the community is placed above the rights of any one individual. This is most clearly seen in the introduction of the idea of a social credit system. Though possibly dystopian to the eyes of a western viewer, many more Chinese people seem fine with the idea of the government having far reaching monitoring powers (Li, 2015).

Considering these backgrounds, we can take a general analysis of these countries' prevailing views and actions. Considering the cultural aspects of Confucianism, privacy was never a large concern in Chinese society. Even recently, cases have been ruled in favor of what benefits the community most over the privacy of an individual. Another aspect of this is that much of the concept of punishment in Chinese culture revolves around the idea of "shame". In this case, the punishment can only occur when wrongdoing is exposed, naturally going against privacy. For this among other reasons, privacy laws have been almost non-existent in China until recently (Li, 2015). This has led to the rapid growth of technology which has little regard for the privacy of the consumer. In fact, privacy is very much a commodity in China now, where bad actors are making large sums of money by hacking into the databases of these data collection companies and selling breached data off by the millions for profit. In this way, one artifact of Chinese culture has caused a negative feedback loop on their views of privacy. Valuing it little has caused bad actors to seize

upon the vulnerabilities and exploit it for personal gain. Following repeated breaches, there has been a new call for stricter punishment and laws against privacy infringement (Feng, 2020).

In the U.S. though privacy has been a fairly universally held value, there are currently few actual laws in place surrounding data collection on the internet. With the rapid development of the internet and technology used for data collection, the legislation has been poor at keeping up. In this case, though the society itself values privacy, a number of factors have led to its disregard. Companies largely collect data from consumers whenever and wherever they can. This can lead to feeling of apathy, such as a large part of America feeling that it is impossible to get through daily life without the government or some companies collecting data on them, while at the same time feeling weary that this data may not be used appropriately or safely (Auxier, 2020). This has led to increased scrutiny over data privacy laws in recent years, and much like China, a call for stricter and more punishing laws against privacy infringement.

Analyzing With SCOT

Analyzing under SCOT, we must first establish relevant social groups. For both countries, this would include, consumers, companies, the government and bad actors (ie. hackers). All have stake in the new technologies which either collect data, or benefit from data collection. Consumers may be considered the source of data, while companies are the collectors and governments are the collectors/utilizers. Bad actors would be considered unintended utilizers as well, a social group which was many do not want to have access.

From there we analyze interpretative flexibility. For the consumers, these technologies used to collect data on them surreptitiously has a wide range of interpretations. In the case of the United States, some do not realize nor care about their online privacy, while others value it greatly

or have been personally affected by some breach of data (Auxier, 2020). Those with strong views for personal privacy are likely influenced by the U.S. culture valuing individual rights and protection from a tyrannical government. These views are also held by consumers in China, however there's a third viewpoint which is held more widely there while only found in a minority of people in the U.S. These are people who support the lack of privacy, specifically around data collection by the government. This subset of the population trusts in the government, believing that the monitoring is for the benefit of a stable society, whether that be to seek out singular criminals, or large-scale organizations. This is a direct parallel to the Confucian ideals which advocate for stability and benefit of the community over the individual's rights (Li, 2015).

For the companies, few data privacy regulations are very beneficial to the bottom line, as they can collect and sell everything they can find with little repercussion or extra overhead to ensure safe standards. This view is held largely by both Chinese and U.S. companies, who have collected data on a massive scale since monitoring tools were first introduced to these new technologies. For any company, the bottom line is the profit they can make, and with the amount of money that can be made using data analysis with few incentives to protect consumer information, there's no reason not to infringe on user privacy. Utilizing consumer apathy, many websites use cookies nowadays, knowing most users won't bother trying to disallow them or otherwise avoid them, simply giving them a brief popup to accept upon navigating to a site. This is one of the primary tools for data collection on the internet, allowing companies to track data and use patterns to individual sessions/devices as they go about their business (Fischer, 2020). There has been no significant push for less data collection outside businesses who make that their primary selling point such as DuckDuckGo, a browser/search system which claims not to track any user data unlike most major competitors. Google and Facebook stand in clear contrast, collecting huge

amounts of data on consumers every day, with few repercussions for data breaches. In 2019 alone, there was a massive breach of over 500 million Facebook users' personal info including names, addresses and phone numbers. However, considering the info was already publicly available, Facebook neglected to even inform potential victims (Bowman, 2021). In China, this rampant neglect for user privacy is even more apparent, where the government actively supports data collection for their benefit. These views by corporations have led to the creation of increasingly complex data collection and analysis tools. In fact, a whole new market has appeared, where some companies' entire business model is collection of user information to be sold to others.

In the case of bad actors, such as individual and state sponsored hackers, there is little difference in opinion. The current state of technology for data collection could not be riper for exploitation. They are also invested in less privacy for the average consumer, so that they can steal and then sell the data that's collected. The lax regulations for and punishments for breaches of user data and privacy has led to little in the way of innovation for safeguards. From here, bad actors create their own technology to help with breaching insecure stores held by companies with massive data on users. In response security companies come up with new ways to make data more secure. This back and forth has become what is known as a digital arms race.

Large differences are mostly seen in the interpretations of each government. In China, the government is largely in support of a lack of data privacy. In fact, many companies have been required to leave in back doors in their technology/applications so the Chinese government can monitor collected data (Khandelwal, 2020). This view specifically has led to one of the most controversial international new stories in recent memory, as the Chinese government begins to experiment with a social credit system. This system would use the various monitoring systems and data collection technologies already in place to aggregate information about a person's actions in

the public sphere and then assign them a social credit score. This score would then be used for a variety of things much like a normal credit score, allowing people who don't disrupt the public more options than those that do. The evolution of this technology is a direct result of their willingness to forgo citizens' privacy in favor of data collection for their own usage. It is also only possible due to the variance in interpretation between nations (Kobie, 2020). While in the U.S. such a technology would face major backlash due to the fundamental belief in extensive individual rights, including privacy, the interpretation in China leans in the opposite direction. As mentioned previously, due to the history of Confucian teachings, Chinese people will often value benefit to the community over rights of the individual, meaning a system where people who commit social disturbances are punished could be welcomed as helping create a more ordered society (Li, 2015). On the other hand, due to significant push from the public to at least place stronger punishments on those who steal various data, there has been movement towards more data privacy laws as the government must at least appease the public. In the U.S. government there are similar viewpoints, while differing in significant ways. Though at times the government believes it should have access to private data, (ex. The incidences in which the U.S. government wanted apple to unlock iPhones/provide a backdoor for the use of the government), it has largely been met with opposition from the public and the court system (Leswing, 2020). Seeing as the U.S. government is meant to be representative of the people, and there has been a large public push for more data privacy after numerous breaches, government opinion has begun turning towards more legislation in recent history (Greenberg, 2020). However, the viewpoints of the U.S. government remained strong, as some policy allows for the legality of mass hacking by the FBI for threats against the nation. This in turn requires advancement of technology to be utilized in these online missions, providing new tools which can breach users' privacy (Sternstein, 2017). These viewpoints show how

governments come to develop similar technologies as they hold similar viewpoints despite coming from differing backgrounds and cultural norms.

In both the cases of the U.S. and China, this new legislation could lead to the rhetorical closure of the current problem. If consumers see that there are less data privacy breaches, or at least lead to believe so, it will begin to be seen as less of a problem. There is also the possibility for redefinition of the problem if modern events change social viewpoints about this particular problem. It could be possible that people stop favoring privacy in order to promote public safety due to some large-scale event or chain of events. In either case, large investment would

Conclusion

Though coming from wildly different backgrounds such as democratic republics/parliaments in the U.S./U.K. and communism in China/Russia, newer societal ideas have begun to take root in response to rapidly developing technology. As data privacy becomes more and more threatened by data collection technologies and bad actors, societal opinions in all countries have begun to shift towards legislation of the issue. Though some will undoubtedly continue to find ways to reduce data privacy for the governments' benefit alone, the general consensus seems to be a reduction of companies profiting off of the people's personal information with zero repercussion for bad practices.

References

Auxier, B., & Rainie, L. (2019, November 15). Key takeaways on Americans' views about privacy, surveillance and data-sharing. Retrieved March 15, 2021, from https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

Bekker, E. (2020, January 3). 2020 data breaches - the most significant breaches of the Year: IdentityForce®. Retrieved March 17, 2021, from https://www.identityforce.com/blog/2020-data-breaches

Bowman, Emma. "After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users." *NPR*, NPR, 10 Apr. 2021, www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users#:~:text=Facebook%20decided%20not%20to%20notify,do%20so%2C%20a%20spokesperson%20said

Feng, E. (2020, January 05). In China, a new call to protect data privacy. Retrieved March 15, 2021, from https://www.npr.org/2020/01/05/793014617/in-china-a-new-call-to-protect-data-privacy#:~:text=Privacy%20becomes%20a%20commodity&text=The%20Chinese%20government%20has%20contradictory,and%20control%20access%20to%20information.

Fischer, Jordan. "Web Cookies and Shadow Data Collection: The Legal Implications." *American Bar Association*, American Bar Association, 6 May 2020, www.americanbar.org/groups/business_law/publications/committee_newsletters/cyberspace/2020/202005/fa_2/

Greenberg, Pam. “2020 Consumer Data Privacy Legislation.” *National Conference of State Legislatures*, NCSL, 17 Jan. 2021, www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx

Khandelwal, Swati. “China Demands Tech Companies to Give Them Backdoor and Encryption Keys.” *The Hacker News*, The Hacker News, 3 Feb. 2015, https://thehackernews.com/2015/02/iphone-china-backdoor.html

Kobie, Nicole. “The Complicated Truth about China's Social Credit System.” *WIRED UK*, Wired, 6 July 2019, www.wired.co.uk/article/china-social-credit-system-explained

Leswing, Kif. “Apple's Fight with Trump and the Justice Department Is about More than Two IPhones.” *CNBC*, CNBC, 16 Jan. 2020, www.cnbc.com/2020/01/16/apple-fbi-backdoor-battle-is-about-more-than-two-iphones.html

Li, T., & Zhou, Z. (2015, January 15). Do you care about chinese privacy law? Well, you should. Retrieved March 15, 2021, from https://iapp.org/news/a/do-you-care-about-chinese-privacy-law-well-you-should/

Pfeifle, S. (2017, September 28). China's evolving views on privacy. Retrieved March 15, 2021, from https://iapp.org/news/a/chinas-evolving-views-on-privacy/

Sharp, Tim. “Right to Privacy: Constitutional Rights & Privacy Laws.” *LiveScience*, LiveScience, 12 June 2013, www.livescience.com/37398-right-to-privacy.html

Sternstein, Aliya. “FBI Allays Some Critics with First Use of New Mass-Hacking Warrant.” *Ars Technica,* Ars Technica, 24 Apr. 2017, https://arstechnica.com/tech-policy/2017/04/fbi-allays-some-critics-with-first-use-of-new-mass-hacking-warrant/