Life, Liberty, and the Pursuit of Digital Sovereignty: U.S. Data Privacy Legislation and Its Conflict Points with the People's Republic of China

Kojiro Matthew Ichida-Marsh

Greenwich, Connecticut

B.A. Italian and Media Studies, University of Virginia, 2023

A Thesis presented to the Graduate Faculty of the University of Virginia in Candidacy for the Degree of Master of Arts

Department of Media Studies

University of Virginia

April 2024

Acknowledgements

First and foremost, I would like to thank my hero and icon, Aynne Kokas, without whom this thesis would not exist. I would also like to extend my sincerest thank you to my committee members, David Nemer and Siva Vaidhyanathan, without whom I would not be able to complete this thesis as well, and whom I appreciate *immensely* for working with me at such a short notice. I would also like to thank the great media studies faculty with whom I've had the privilege of working, such as Elizabeth Ellcessor, who helped me through the worst times of the thesis writing process.

On a more personal note, I would like to thank my friends and family for their emotional support along the way. I would like to say thank you to my family; Ryan, Kiyana, and my mom and dad for all of their emotional help throughout this journey and life. I would also like to thank so many of my friends from my year as a master's student for motivating me to go to the library; Callie Barr, Chase Candeloro, and Ami Suchdev thank you for that. Thank you to John Wallace, Andrew Kent, and Liam O'Donnell for dealing with my shenanigans throughout this year on the home front. Lastly, I would like to thank JunJun Yu, my favorite librarian ever, who helped me get into the right mindset each and every morning!

Table of Contents

Introduction: United States Views of Data Privacy

The U.S.'s "TikTok" Problem

"Let me state this unequivocally: ByteDance is not an agent of China or any other country," TikTok CEO, Singaporean national Shou Zi Chew, claimed about their parent company in March of 2023.[1] The Congressional hearing in front of the United States House of Representatives' Energy and Commerce Committee was called "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms."[2] This was a rare bipartisan effort in the U.S. Congress that addressed a myriad of issues relating to the social media app. While child safety, Spanish-language prioritization, addiction concerns, and racist implicit bias embedded in the algorithm were all areas of concerns from the members of Congress, there was ultimately one matter that stood out among all of them: national security concerns as it relates to TikTok's parent company, ByteDance.[3] While Shou Chew tried to separate TikTok from its Chinese-owned parent company, and from TikTok's mainland Chinese counterpart, Douyin, every member of the Congressional committee was relentless in their questioning of the safety of Americans using the popular social media application, at the time used by over 150 million people in the United States.[4] This is not the first time that the United States Congress has discussed data privacy and data security for American citizens, but this is the first time that it had a major international social media company at the center.

---

[1] *TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms*, House of Representatives Energy and Commerce Committee, 2023, https://www.c-span.org/video/?526609-1/tiktok-ceo-testifies-house-energy-commerce-committee-hearing.
[2] Ibid.
[3] Ibid
[4] TikTok Team, "Celebrating our thriving community of 150 million Americans," TikTok, March 21st, 2023, https://newsroom.tiktok.com/en-us/150-m-us-users

The following thesis intends to inform the discussion of data privacy as it relates to international social media companies, particularly Chinese-owned ByteDance's TikTok, through the analysis of first of the concept of the idea of data privacy, which then leads into a broader discussion of what the implications are for so many U.S. citizens to be using an app that is owned by a Chinese company. Ultimately, this thesis intends to better advise conversations about what the data privacy legislation looks like in the United States, and what models we can use to better protect digital sovereignty.

I argue that the way in which the current privacy landscape is set up in the United States allows social media companies like TikTok to exploit user data for profit. This becomes especially problematic when companies like TikTok operate on an international level, especially as foreign adversaries are keen on obtaining U.S. citizens' information. Using an analysis of various legal documents relating to U.S. privacy, I first expose the policy gaps in the legislation that allow user data to be extracted legally. After this, I look at the Commonwealth of Virginia as a case study example of what effective privacy policy governance looks like in an American context, while also paying close attention to the negative ramifications of laws that are too stringent, which can stifle education and commerce. Lastly, I investigate how the TikTok has found itself in the middle of the data sovereignty battle between the United States and the People's Republic of China. I hope to explain in this thesis that there is potential in the United States for a comprehensive data privacy regulation and to prevent the dangers of international companies from preying on user; all we must do is look at Virginia.

TikTok

TikTok is a video sharing app owned by ByteDance, a company based out of Beijing, China. While many compare the app to Vine, its predecessor in the United States is Musical.ly,

which was purchased and merged with TikTok,[5] ByteDance's foreign version of their native Douyin. Especially after the shutdown of Vine, it quickly became the fastest growing social media app in the world and in the United States alone, there are over 150 million users, most of whom are youth.[6] During the COVID-19 lockdown and pandemic, TikTok became critical infrastructure for millions, as many used it as an outlet during the stressful times.[7] Klug, Kaufman, and Evans use a uses and gratifications theory approach to explain this phenomenon of TikTok replacing many social interactions and being a place for mutual support, coping, and understanding.[8]

Because of this critical mass that TikTok has reached, many politicians have concerns related to its privacy from a national security perspective, among a host of other issues such as implicit bias built into its algorithms, spreading of false information, and promoting harmful content.[9] In the United States, the first official motion into the potentiality that TikTok could be a national security threat came in October of 2019, when US intelligence officials were asked by Congress to investigate if TikTok posed any national security risks.[10] By December of that year, the US army had banned the use of TikTok on any government issued phones, while also urging

---

[5] Joe Tidy and Sophia Smith Galer, "TikTok: The Story of a Social Media Giant," BBC, August 5th, 2020, https://www.bbc.com/news/technology-53640724,

[6] TikTok, "Celebrating our thriving community of 150 million Americans."

[7] Zongyi Zhang, "Infrastructuralization of Tik Tok: Transformation, power relationships, and platformization of video entertainment in China," *Media, Culture & Society* 43, no. 2 (2021): 219-236

[8] Klug, Daniel, Morgan Evans, and Geoff Kaufman, "How TikTok served as a platform for young people to share and cope with lived COVID-19 experiences," *MedieKultur: Journal of media and communication research* 38, no. 73 (2022): 152-170

[9] *TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms*, House of Representatives Energy and Commerce Committee, 2023.

[10] Katie Elson Anderson, "Getting Acquainted with Social Networks and Apps: It Is Time to Talk about TikTok," *Library Hi Tech News* 37, no. 4 (2020): 7–12.

many others not to use it due to privacy concerns.[11] After this, TikTok was treated as a legitimate national security threat.

On August 6, 2020, then President Donald Trump issued an executive order to combat Americans from downloading apps that are developed and owned by companies that are based out of the People's Republic of China.[12] Citing national security concerns, Trump gave ByteDance 45 days to find a buyer for TikTok.[13] Bans of this application had already been executed in other countries throughout the world at the time, such as in India.

In 2024, the state of TikTok is very much still in the air. While there have been individual states who have banned TikTok in varying degrees (e.g. banning them simply on government-issued devices), national bans are still not out of the question, as will be explored later in this thesis.

Overall, it is essential to understand the origins of where TikTok came from to better understand many concepts that continue in this thesis. While, for example as later explored, TikTok's privacy policies are not as aggressive as say, Instagram's privacy policy, its foreign implications are a large reason for why the C.E.O. was called in to testify before the United States Congress. In addition to this, it is essential to understand how TikTok has come to be such a large player.

The *Oikos* Versus The *Polis*

Throughout this thesis, the word "privacy" is used quite often. However, as explored in the following section, conceptions of privacy vary from culture to culture, and are often very

---

[11] Ibid.
[12] Younghoon Chang, Siew Fan Wong, Christian Fernando Libaque-Saenz, and Hwansoo Lee, "The role of privacy policy on consumers' perceived privacy," *Government Information Quarterly* 35, no. 3 (2018): 445-459.
[13] Ibid.

specific to the ones to whom it applies. The Western concepts of privacy are ultimately the study of this thesis, and the definitions of privacy play a foundational role in data privacy, which ultimately is a critical aspect of digital sovereignty.

The primitive and innate concept of privacy is older than human civilization, according to famous anthropologist Margaret Mead.[14] Contemporary American conceptions with which this text intends to interact and off of which it builds, stem from a long lineage of Western classical liberal thought. While ultimately engaging with Aristotle's idea of private life (the *oikos*) as a necessitating a physical "sphere," the modern perception of privacy begins in the 18th century.[15] During this time, Enlightenment thinkers theorized that privacy is *contradictory* in nature, in the sense that it must define itself using the context of social interaction with the community (the *polis*), despite being the absence of this form of communication.[16] Privacy during the time of the Enlightenment was considered a freedom from the powers of external intervention via surveillance by authorities or individuals whereby one holds personal interest against that of the larger social group.[17] The connotations of privacy, however, vary widely between cultures, with several not even having a remote translation for this foreign concept.[18] This goes to show that ultimately, the idea of privacy varies on the context in which it finds itself, so it is important to note that we are talking about specifically Western conceptions of privacy.

---

[14] Margaret Mead, "Neighborhoods and human needs," *Children's Environments Quarterly* 1, no. 4 (1984): 3-5.
[15] Jim Roy, "Polis and Oikos in Classical Athens1," *Greece & Rome* 46, no. 1 (1999): 1-18.
[16] Benoît Melançon, "L'invention de l'intimité au Siècle des lumières," (*Centre des Sciences de la Littérature Université Paris X - Nanterre*, 1995), 5-22.
[17] Sabine Trepte and Philipp K. Masur, "Introduction," in *The Routledge Handbook of Privacy and Social Media*, (Routledge, 2023), 3-15.
[18] Margaret Mead, "Neighborhoods and human needs," *Children's Environments Quarterly* 1, no. 4 (1984): 3-5.

A further fundamental exploration of the concept of privacy as it relates to democratic societies arose in 1967 with Alan F. Westin's release of *Privacy and Freedom*.[19] Westin conceptualizes privacy as it pertains to contemporary American life and Western democracies as being the self-determination of the dissemination of intimate information to others.[20] He also posits that privacy is necessary in preserving individual freedom in a society. The key piece of understanding here is that it is ultimately the *choice* of the individual whose data it is as to where this data will go.[21] With this concept of choice, also comes the idea that an individual has some sense of *control* or *ownership* over their information.

Despite attempts from these nebulous definitions, core characteristics of privacy have been historically difficult to identify. Privacy, according to contemporary thinker Daniel Solove,[22] cannot be defined by fundamental elements, rather it should be conceptualized as being uniquely formulated and delineated via the happening of particular circumstances that suggest our preconceived notions of it have been violated.[23] As did Westin, Solove emphasizes the heterogeneity in connotations of privacy across societies and time in directing thinkers to the conclusion that privacy is ultimately contextual.[24] In pursuit of balancing the flexibility of accommodation and usefulness of stability, Solove proposed a *taxonomy*, rather than a definition, of privacy; a framework through which to view the diverse contextual forms of privacy.[25] Solove thus takes a firm stance as an anti-reductionist viewer of privacy, which emphasizes a pluralistic understanding. Thus, privacy is too complex to define as a concrete unit of language and rather

---

[19] Alan F. Westin, *Privacy and Freedom*, Atheneum, 1967.
[20] Ibid.
[21] Ibid.
[22] Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008).
[23] Ibid.
[24] Ibid.
[25] Ibid.

should be understood as a multifaceted and adaptable nomenclature of related theories.[26] In the context of this thesis, this is important to understand as privacy can change depending not only on the context of the society within which it finds itself, but also even varies in interpretation within specific situations. Ultimately, by understanding privacy as a taxonomy, we can better understand the idea that privacy is multifaceted in nature and requires different contextual clues to fully determine the violation of a person's privacy.

Ultimately however, according to Westin, humans seldom crave unconditional privacy because of the innate individual desire to participate in society, which requires conceding personal information.[27] The spectrum of compromise ultimately is an adjustment process in which the individual negotiates the desire for insulation with that of inclusion through divulgence.[28] Modern privacy theorists evaluate the role of rational decision-making in calculating perceived risks and rewards and how this affects behavior. From this, theorists divide into two main camps: those who believe that individuals engage in a purely rational cost-benefit analysis and those who believe that individuals resort to heuristics, or bounded rationality.[29] It is essential to understand that no society can function with complete privacy of individuals. Some information must be given up to participate within a society, but there are various characteristics that can determine whether or not a person chooses to actually engage. Thus, there is no real argument for why people cannot stop the leakage of massive amounts of their personal data, because of the necessity to interact with and live in a functioning society.

---

[26] Ibid.
[27] Westin, *Privacy and Freedom*, Atheneum, 1967..
[28] Ibid.

[29] Natalie N. Bazarova and Pengfei Zhao, "Individualistic Privacy Theories," in *The Routledge Handbook of Privacy and Social Media*, (Routledge, 2023), 16-24.

In terms of understanding privacy for the purposes of this thesis, there are a few critical takeaways from this section. The first is that there is a long lineage of the history of privacy in Western thought, as well as specifically in the United States, which ultimately point to the fact that every society has a unique relationship with this concept. In addition to this, it is a complex and often disagreed upon concept, about which even major theorists do not show consensus. Lastly, while there is no one correct reason for why any given individual cedes their privacy, ultimately it is the choice that the individual has that determines whether there has been an invasion of their privacy.

Privacy Policies

Ultimately these conversations about privacy lead into conversations surrounding what exactly the consent procedures are for giving up one's privacy. If it is essential that any given person must consciously choose whether or not to give up their privacy, then it must be necessary first for them to understand the conditions under which they are conceding it. In this sense, for the purposes of better understanding the situations into which people have been put when interacting with the world around them, especially online, privacy policies need to be better understood. In addition to this, later in this thesis, TikTok's privacy policy will be explored to see how it holds up to the U.S. conception of the taxonomy of privacy.

The concept of a "privacy policy" stemmed as a reaction to the sentiment that many people felt when they were giving massive amounts of their personal data to large internet-based companies. In the United States, as of the Privacy Act of 1974, which has since been amended and will be further explained in Chapter 1, most companies are required to disclose some sort of privacy policy to their consumers, for the purposes of protection and consent.[30] Even when

[30] Act, Privacy. "Privacy Act of 1974." (2019).

people have access to this information, however, does not necessarily mean that they take it into account when using the internet. It is because of factors such as these that it is important that the government gets involved to regulate the actions of larger corporations who are collecting information.

To better understand online privacy and why people continue to interact with the internet sometimes despite their own best intentions, it is essential to understand Sandra Petronio's communication privacy management theory (CPM).[31] CPM theory further expands on Westin's idea of a spectrum, by delineating open boundaries (willing concession of information) in contrast to closed boundaries (protection of information). Individuals require consistent adaptation to levels of disclosure to accommodate social needs with that of personal autonomy.[32] Privacy rules dictate the level of privacy, which consider the degree of boundary permeability with that of relationships with others.

CPM theory helps better understand why people choose to sometimes give up their privacy online. There are four important concepts that are essential in the conceptualization of CPM: people believe that they own the right to their personal information, people use their own rules to control their information, people "co-own" information, and chaos can follow the lack of understanding between co-owners. When trying to understand why there is such a large conflict between users and social media companies at the moment, it is essential to grasp these concepts. People believe that they own their own information, which makes it inherently a conflict to them when it gets exploited or used in ways for which it was not intended. This is one of the most critical points to understand about privacy explained in the introduction. The idea that ultimately,

---

[31] Sandra Petronio, "Communication privacy management theory: What do we know about family privacy regulation?," *Journal of family theory & review* 2, no. 3 (2010): 175-196.
[32] Ibid.

there are questions of ownership involved with privacy, as well as the idea that misuse of it in any way can be a way in which privacy can further be delineated.

In the larger case of TikTok, the United States, the People's Republic of China and digital sovereignty, people have become upset when what they are consenting to does not line up with what is happening in actuality. While this will be expanded upon further in the following chapters, essentially the Chinese government has the ability to access data via TikTok, which isn't necessarily to what users of the social media platform have explicitly consented.

There is much literature surrounding the idea of privacy policies specifically, such as Candice Hokey and her instrumental paper entitled "Are They Worth Reading? An In-Depth Analysis of Online Reading? An In-Depth Analysis of Online Trackers' Privacy Policies."[33] This text delves into the idea of whether the information contained in privacy policies is appropriate for what is needed for people to properly consent. Using an analysis of privacy policies, Hokey expresses concern about the ways that privacy policies are intentionally vague so that they may take more information while still being "compliant."[34] In addition to this, much information is left out or left vague, such as who is "we," in the context of a privacy policy document[35] (e.g. does "we" include the government of the country in which the specific enterprise is based?). Ultimately, this is because large companies have an incentive to collect as much data as possible from someone because of the non-depleatable nature of data.

Many privacy policies in the United States are based around the Federal Trade Commission's five "fair information practices," which are notice, choice, access, security, and

---

[33] Lorrie Faith Cranor, Candice Hoke, Pedro Giovanni Leon, and Alyssa Au, "Are they worth reading-an in-depth analysis of online trackers' privacy policies," *ISJLP* 11 (2015): 325.
[34] Ibid.
[35] Ibid.

enforcement.[36] Notice refers to the necessity to be notified of practices, choice is the option of how to use personal information, access refers to the ability for users to self-verify information, and security means that the data must be secure.[37] Ultimately, however, these privacy policies have been created by and for social media companies and their protection, and as we will see later on in this thesis, there are many different ways in which the information in privacy policies can be used.

Big Data

The last essential concept which will be discussed in the introduction is Big Data, which is important because of the fact that in aggregate, data becomes much more powerful than its pieces. While it is easy to dismiss the ideas that one's data being collected is not much of a problem (e.g. when people respond to having their data collected with something along the lines of "What would anyone even want to/could do with my TikTok dance video preferences?" or "I'm not important, I don't care who has my data!"), it is important to note the differences between one person's data and the collection of millions or even billions of people's data. It is also essential to understand that massive amounts of data collected about you could put people in your data periphery, so to speak, in situations that *they* would not prefer.

The early 2000s brought about the term "Big Data," to accommodate the concept of the new massive volume of information that no longer fit into the memory of single computers.[38] Big data affords the extraction and creation of new value, which would otherwise be

---

[36] Fair Information Practice Principles (FIPPs), U.S. Federal Government, 2022, https://www.fpc.gov/resources/fipps/
[37] Ibid.
[38] Sagiroglu, Seref, and Duygu Sinanc. "Big data: A review." In *2013 international conference on collaboration technologies and systems (CTS)*, pp. 42-47. IEEE, 2013.

insurmountable.[39] This goes to show that many people's data collected together can be much more powerful in whole than the individual parts. For example, if someone looks up information about their diabetes, it might not be important to a foreign adversary. However, if say, 200 million American citizens all looked up information about their diabetes, there could be a pretty solid picture painted of the overall health of a nation.

In addition to the risks of foreign powers having access to massive amounts of data, new Big Data processing technologies were propelled forward by companies who now stored costly multitudes of data looking to utilize it for profit, thus intrinsically linking it to the extraction and commodification of human information.[40] Essentially, the origins of Big Data were a matter of exploiting consumers in every aspect for fiscal gain. From this, comes the idea of surveillance capitalism, which intends to predict and control human behavior.[41] Modern digital surveillance capitalism is unique in that it is structurally independent from the users from whom it collects data. Ultimately, the scholar who coined the term "surveillance capitalism" in 2015, Shoshana Zuboff, emphasizes how this creates a "Big Other," which is an invisible, omnipresent surveillant with the ability to control individuals' actions through leveraging of users' data. Unlike traditional power structures, the Big Other relies on data and algorithms, thus shifting humans away from the social contract towards an automated system.[42] Why it is important to understand how Big Data has led to surveillance capitalism is because ultimately the United States is a capitalist country. Because of this, it is very reasonable to assume that there are massive amounts of data being obtained on U.S. citizens in the 21st century. Even worse than

---

[39] Ibid.
[40] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data*, (Houghton Mifflin Harcourt, 2013), 6-7.
[41] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (2015): 75-89.
[42] Ibid.

this, foreign adversaries like the People's Republic of China have similar access to this massive amount of American data, which they can use to influence the U.S. extraterritorially. Thus, big data and the surrounding concepts have massive implications for the digital sovereignty of a nation.

Data itself is diverse in type, with there being a spectrum of structured, semi-structured, and unstructured data, which refers to whether the information is well-defined within set parameters (e.g. a spreadsheet) or more abstract (e.g. a video). Unlike other commodities, data is infinitely reusable and non-depletable. Because of this, some argue that data is even more lucrative than traditional industries such as oil or coal whose raw materials can be exhausted.[43] This is one of the ways in which some social media companies and data brokers have become so large, because of the fact that they can sell data to virtually unlimited buyers. While this thesis mainly interacts with the People's Republic of China as the United States' main foreign adversary, it is important to note that there are farther reaching implications of big data and surveillance capitalism than what is explored here.

2011's "Critical Questions for Big Data" depicts Big Data as a phenomenon that results from the interplay of technology, analysis, and mythology the former two of which seek the maximizing of computational power and algorithmic accuracy and identifying applicable patterns, respectively.[44] The recognition of the mythologizing of Big Data is an essential primary key to understanding what Big Data is not: perfect, objective, and esoteric. This last point offers

---

[43] Hirsch, Dennis D. "The glass house effect: Big Data, the new oil, and the power of analogy." *Me. L. Rev.* 66 (2013): 373.

[44] Danah Boyd and Kate Crawford, "Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon," *Information, communication & society* 15, no. 5 (2012): 662-679.

the reader access to this otherwise unapproachable topic and argues that understanding that big data is not impossible to comprehend and should be attempted to be comprehended.[45]

Positionality

As I write this thesis, I am a current master's student at the University of Virginia, where I also received my undergraduate degree in May of 2023. Because of this, I have been experiencing the constant changes that have been going on in the United States, and specifically the Commonwealth of Virginia in the last few years. My time at the University of Virginia has best equipped me with the knowledge and tools necessary to conduct a piece of research such as this. Not only have I assisted in some of the research under renowned professor and scholar Aynne Kokas as she finished her second book about Chinese data trafficking of U.S. data, but I have also been involved with events around the University of Virginia campus. One of such events was a talk at U.Va.'s Miller Center for Politics, which brought in a Virginia state senator to talk more about some of the specific pieces of policy that have been passed recently that pertain to digital sovereignty and data privacy. While I cannot discuss the specifics in this thesis, I learned much about the way in which we talk about data privacy on a state level from events such as these. In addition to this, through my master's level coursework, such as taking classes like Computational Media, Data and Democracy, and Social Media Methodologies, I have found that I have become uniquely positioned as a scholar to examine the ways in which data privacy and digital sovereignty can drastically affect the world around us.

[45] Ibid.

Methods

The following thesis will use a variety of methods to better understand and explore the ideas around TikTok, data privacy, and ultimately data sovereignty. Textual analysis is the main way through which a variety of documents will be analyzed, however there are three methods that will be used. The two in addition to textual analysis are an auto-ethnographical section and two comparative analyses.

The first chapter will look into various documents that have been released by the Supreme Court to best explain their rulings, as well as acts and laws passed in the United States by the federal government that pertain to privacy. While I am not a legal scholar, I attempt to best elucidate what exactly many of these U.S. privacy laws and arguments mean for the everyday American who is online. Ultimately, the document analysis will be done to further the argument that the United States does not have strong enough protections for its citizens' data being poached by private corporations and the dangers that this poses.

The second chapter starts off similarly to the first chapter in its exploration of various legal documents. However, in this second chapter, the main focus is around specifically the Commonwealth of Virginia. Alongside the document analysis, there are two studies that have been conducted that relate to the way that Virginia is going about protecting the data privacy of their citizens. The first study is an autoethnographic study on the impact that some Virginia laws have on small business owners who are attempting to come into compliance with them. The second study is a specific case study looking into the University of Virginia, the premier public university in the Commonwealth of Virginia, in order to best understand how these laws are affecting educational institutions.

Lastly, the final chapter will be a document analysis as well as a comparative analysis of three different points of view. Firstly, documents will be analyzed that explain the point of view

of TikTok on being caught in the middle of a Sino-American war on data sovereignty. Documents will then be compared with the perspectives of the Americans, specifically the House Democratic Committee on Energy and Commerce. Lastly, Chinese laws and responses to TikTok and data sovereignty will be explored and compared to the ways in which American laws function and how their laws interact with private enterprises like TikTok's parent company, ByteDance.

Structure

The structure of the thesis will be divided into three chapters, which all intend to ultimately interact with the ideas of data privacy and data sovereignty and what these look like in the United States as they pertain to the Chinese ownership of TikTok's parent company. In this, I argue that there are not sufficient policies in place on a federal level in the United States to properly protect its citizens from the dangers of the Chinese Communist Party's obtention of their data. I argue that without a comprehensive digital privacy framework in place, Americans are at risk of private enterprises being able to freely collect their data and use it in any way in which they choose. I argue that there is a way in which the United States can remedy these problems by looking at individual states like Virginia who have created a solid digital privacy law within the context of an American democratic, capitalist, and overall cultural system. In essence, the United States unfortunately does not have a comprehensive federal data privacy legislation despite one existing in various states, like Virginia, who could inform what this should look like. Ultimately, this leaves U.S. users in danger of losing their data privacy to foreign adversaries like the People's Republic of China via private companies like TikTok, thus affecting our digital sovereignty.

The first chapter is entitled “The American Data Wild West and the Data Mining Goldrush.” This will explore rulings passed by the Supreme Court of the United States that have to do with privacy, which helps best understand what the legal definition of privacy roughly is in the United States, as there is not one clear definition. In addition to doing a close analysis of various Supreme Court rulings, the first chapter will explore various laws that are in line with this idea of privacy in the United States, to see not only what the understanding of privacy is, but also how this is applied to the everyday lives of hundreds of millions of Americans. Laws that are created expressly to protect the privacy of individuals will be explored alongside a few that many argue infringe on many of the privacy rights. Ultimately, the purpose of this chapter is to better understand the current landscape of privacy in the United States so that the role of social media companies and other large data brokers can be better explored. In this chapter, it is argued that there is not sufficient enough data privacy legislation in the United States at a federal level to protect all of its citizens.

The second chapter of this thesis, “Virginia Is for Data Privacy Lovers” looks into the Virginia laws that have been put in place to protect consumer privacy. By looking into first laws like the Virginia Consumer Data Protection Act, we can better understand what a uniquely American view on data privacy would look like in the 21st century. Alongside this, however, I also intend to highlight some of the negative aspects that come along with further regulation of data. While I argue that laws like these are necessary, I find it important to acknowledge ways in which the laws are not perfect. Ultimately, I find that these negative aspects to not outweigh the pros of having a piece of legislation like this in place. In a similar vein, I look at how laws like those banning foreign companies like TikTok are good in many ways, yet still have some negative ramifications. Ultimately the purpose of this chapter is to better inform what a

comprehensive data privacy environment looks like at a smaller level in the United States, while also pointing out the areas of imperfection. The second part transitions from data privacy, to how this data privacy has an effect on digital sovereignty. These two are very much connected because of the fact that digital sovereignty cannot be established without first having concrete data privacy and data security laws in place.

The final chapter is a culmination of many of the ideas that have been built up in the first two. While looking at how the United States does not have proper measures to protect its citizens from private companies exploiting user data, I look into how this is dangerous on an international level as it relates to the People's Republic of China and TikTok's parent company. Laws like the ones in Virginia are ultimately created not only to protect the consumer, but to create a sense of digital sovereignty. I argue that without proper measures in place on a federal level like there are on a state level in Virginia, the Chinese Communist Party has almost free reign over access to U.S. citizens' data. I use TikTok as a case study in this final chapter to explore this concept. While TikTok is operating well within its legal limits in the United States, they are also beholden to many of the dictatorial policies found in the People's Republic of China. The P.R.C., as explored in this final chapter, has many ways in which it can force multinational companies into ceding data into their hands. This last chapter essentially explains why the precarious situation explored in Chapter 1 is so precarious. Not only can companies exploit massive amounts of user data from Americans, but the companies can also sell this data to foreign adversaries like the People's Republic of China. In order to best protect against situations like these, it is essential that pieces of privacy legislation like those found in the Commonwealth of Virginia are implemented in some way on a national scale in the United States.

Overall, this thesis' goal is to explain the current situation in the United States on a national level, explore why this is a dangerous situation in which to be considering the Chinese Communist Party-led government is hungry for American data, and what a possible way to prevent the transfer of U.S. data into the hands of our foreign adversary is.

Chapter 1: The American Data Legislation Wild West and the Data Mining Gold Rush

Introduction

After understanding exactly what data privacy is, it is essential to understand how this practically applies to the everyday. For example, currently in the United States on a federal level, there are very specific limits as to what is *explicitly* protected under the general legal umbrella term of "privacy." In order to best respond to the question of the applicability of theories of privacy translated to the real world, the U.S. Supreme Court has a long history of explaining the complex and vague concept "privacy," which eventually gets further delineated via various acts passed by the U.S. Federal Government since the 1970s. While data leaks and hacking are still serious concerns, much of U.S. citizens' data can actually be accessed and stored relatively easily. Ultimately, these acts show the vulnerability of U.S. user data can lead to the exploitation of information by both the federal government and private companies operating in the United States. It is important in reading this to understand the differences also, between data privacy and data security. While both of these terms ultimately work towards the goal of protecting the integrity of an individual's data, they differ in their approaches and meanings.

These ideas in the first chapter ultimately intend to inform larger questions of what is happening with U.S. citizens' information and data, and what are the national security implications of having such lax data privacy laws. By first understanding the differences between data privacy and data security, this chapter will then attempt to better understand the data privacy landscape in the United States as of March of 2024. In order to best do this, it is necessary to understand the origins of the legal definitions of privacy in the United States, as delineated by the Supreme Court. After a close reading of the ways in which privacy interacts with the

Constitution of the United States, the concept of privacy can best be understood in a federal context. From this, close readings will be done with essential acts passed by the United States Congress which interact with this idea of "privacy" as a central point. First, acts that are aimed at protecting "personally identifiable information" will be explored to see the stringency of U.S. law. Of the many that have been proposed in the United States the ones being explored are the Information Sharing and the 2002 Health Insurance Portability and Accountability Act (HIPAA) and the 2008 Children's Online Privacy Protection Act, which are the two most relevant and critical pieces of legislation. After this, there are a series of acts passed in the United States at a federal level that, in certain interpretations of privacy, infringe on the rights of U.S. citizens. Of these, the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," commonly known as the USA PATRIOT Act, or simply, the PATRIOT Act, will be the first and most major act to be explored. In the wake of this watershed act, the 2002 Homeland Security Act and The Foreign Intelligence Surveillance Act will be explored to see how they interact in similar ways and expands the powers of the USA PATRIOT Act.

After the picture has been painted of the current privacy landscape in the United States, private social media corporations will be explored as one of the main exploiters of U.S. citizens' data. This chapter intends to argue that the lax laws that have been implemented on a federal level ultimately lead to the abuse of U.S. citizens' data, and data breaches and close relationships with the U.S. federal government have ultimately led to a Wild West situation.

Data Privacy Versus Data Security

Data privacy can best be summed up as the right to be left alone,[46] wherein the user has the ability to choose by whom their data is being accessed and stored, and to a certain extent, how it is being used. Data privacy thus focuses on the *governance* of the use of user data. This is the main discussion about which the following chapter and thesis intends to inform.

While closely related, data *security* explains the concept of how secure one's data is after the user has consented to give them to any given organization. Essentially, data security focuses less on policies that protect users from being exploited, and more so on protecting the data that has been given consensually. In this sense, data security is a critical piece of data privacy in its ability to help users maintain their control over their information. If data security is not first established, there is no way to guarantee that there will be any sense of data privacy because of the risk of unauthorized access.

Legal Definitions of Privacy in the United States

In order to best understand the legal foundations for privacy law in the United States, it is most essential to understand a select few amendments, namely the First, the Third, the Fourth, the Fifth, the Ninth, and the Fourteenth. While there is no direct mention of the word "privacy" in the U.S. Constitution, over the past century, these six amendments have been interpreted and expanded in scope to protect U.S. citizens' privacy, especially when interacting with the government. These amendments are ultimately the basis for the fundamental ways in which the United States federal government views the rights to privacy of its citizens. Because of the fact that the Constitution is the document on which current privacy legislation is based and judged, it

[46] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890): 193-220.

is foundational in the better and more comprehensive understanding of current United States privacy policies. Regardless of policy agendas of congresses or presidents, the Constitution is unchanging and restrictive in its permission to infringe on its delineated rights.

The origins of privacy law in the United States is largely agreed to have started in the late 1800s. The right "to be let alone" in the United States was born with Samuel D. Warren and Louis D. Brandeis' law review: *The Right to Privacy*.[47] As explored by Warren and Brandeis, modern enterprise and invention had led to the invasion of the individual's privacy, which they define in part as the exclusive authority to fix limits on personal publicity.[48] Even from the origins of this concept in the United States, we can see that the sense of control or ownership has become a major part of a definition of privacy. To this day, this article is considered to be one of the most fundamental and foundational pieces of legal literature surrounding privacy laws in the United States.

One of the first cases in the United States that directly dealt with U.S. citizens' right to privacy was the 1928 ruling in *Olmstead v. United States*. While ultimately this did not rule in favor of the individual whose privacy was allegedly being violated, it was nonetheless important in its use of the Fourth and Fifth Amendments for the establishment of a then nebulous concept of privacy. In this case, the Fourth Amendment's "search and seizure" clause was used in a literal sense, therefore not being violated in a case wherein wiretapping was used to "search."[49] The Fifth Amendment was also established as a fundamental amendment in this case, but again it was not violated, as then Chief Justice and majority opinion-writer William Howard Taft ruled

---

[47] Ibid.
[48] Ibid.
[49] William Howard Taft and Supreme Court Of The United States, U.S. Reports: Olmstead v. United States, 277 U.S. 438, 1927, Periodical, https://www.loc.gov/item/usrep277438/.

that this was not a case of self-incrimination.[50] An important note in this court ruling was that there is an established difference between something being unethical and unconstitutional. While in this court case, Taft recognizes that the evidence in this case was procured "unethically," it still was still ruled to be constitutional.[51]

Ultimately, this case was overturned in 1967 with the ruling of *Katz v. United States*, which importantly rejected the literal understanding of the Fourth Amendment, specifically dealing with, again, the "search and seizure" clause.[52] In this case however, the federal government's use of wiretapping on a public phone booth, majority opinion Potter Stewart concluded, violated a constitutionally protected "reasonable expectation of privacy."[53] The concept of a "reasonable expectation of privacy"[54] is further expanded upon in the concurring opinion written by John Marshall Harlan II, which importantly creates the concept of the "Katz Test." The "Katz Test" establishes whether or not there exists this "justifiable" expectation of privacy, thus showing that privacy in the United States is situational.[55] This shows that in the United States there are different contexts for whether information is considered to be "free reign" in a sense.

The most important case in the modern U.S. understanding of privacy comes with the Supreme Court case *Griswold v. Connecticut* in which the majority opinion, written by William O. Douglas, establishes that the First, the Third, the Fourth, the Fifth, and the Ninth Amendments together create a very important legal concept in constitutional law called a "penumbra," which

---

[50] Ibid.
[51] Ibid.
[52] Potter Stewart and Supreme Court Of The United States, U.S. Reports: Katz v. United States, 389 U.S. 347, 1967, Periodical, https://www.loc.gov/item/usrep389347/.
[53] Ibid.
[54] Ibid.
[55] Ibid

derives rights from implications found in the Bill of Rights.[56] In *Griswold v. Connecticut*, Douglas establishes that in using penumbral law, the general right to privacy can be inferred from those amendments.[57] The following section from the case authored by Douglas explains the amendments from which the privacy penumbra can be derived.

> The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment, in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner, is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment, in its Self-Incrimination Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.[58]

While each of these amendments are critical in the foundations of a U.S. right to privacy, Douglas critically includes the “forgotten” Ninth Amendment.[59] By including an additional amendment into the penumbral law, Douglas is able to further the case for privacy being implicitly derivable from the Constitution.

Overall, privacy has been interpreted by the Supreme Court of the United States in various scenarios. While there are trends as to which amendments are most closely linked to the idea of privacy, “privacy” is not mentioned in the U.S. Constitution, and is thus not an explicitly

---

[56] William Orville Douglas and Supreme Court Of The United States, U.S. Reports: Griswold v. Connecticut, 381 U.S. 479, 1964, Periodical, https://www.loc.gov/item/usrep381479/.
[57] Ibid.
[58] Ibid.
[59] Ibid.

given right to any U.S. citizen. This is fundamental in understanding why the United States deals with data privacy in the way it does. Without any definite mention of privacy, there is no pressing need or will for the federal government to protect it.

Federal Acts That Protect Personally Identifiable Information

Unlike the Norway or Japan, the United States does not have a comprehensive national law that aims to protect the privacy of private citizens. Throughout the history of the United States, however, there have been various acts that either better protect and infringe on personal privacy; the following three sections explore former. Overall, I intend to explore how despite there is a framework that exists in the United States that deals with privacy. It is also essential to note in the following sections the limitations of the already limited privacy policies set forth on a national level in the United States.

Starting in the 1970s, the U.S. began to pass important acts that dealt with what is referred to as "personally identifiable information" on private citizens. *The Privacy Act of 1974* establishes this concept, henceforth abbreviated as "PII," and how the federal government handles, disseminates, maintains, uses, and collects this information. Importantly under this act the "Fair Information Practice Principles" (FIPPs) that are used by federal agencies "when evaluating information systems, processes, programs, and activities that affect individual privacy"[60] was established. It is important to note about these principles, however, that they are at best suggestions for ways in which government agencies *should* handle PII "according to the agency's particular mission and privacy program requirements."[61] While important in a better

[60] Federal Trade Commission, Fair Information Practice Principles, December 29, 2008, https://www.fpc.gov/resources/fipps/
[61] Ibid.

understanding of the ethical framework of the U.S. Federal Government as it pertains to privacy, as Taft stated, the law and ethics don't always align perfectly.

There are nine different principles, which include "Access and Amendment," "Accountability," "Authority," "Minimization," "Quality and Integrity," "Individual Participation," "Purpose Specifications and Use Limitations," and "Security." The following table summarizes the terminology used to define protected privacy.

Access and Amendment. Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.	**Accountability.** Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.	**Authority.** Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.	**Minimization.** Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.	**Quality and Integrity.** Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
Individual Participation. Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.	**Purpose Specification and Use Limitation.** Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.	**Security.** Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.	**Transparency.** Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.	[62]

These definitions are critical for understanding the way in which the privacy system works in the United States. Many of the ways in which privacy policies even at private enterprises are created involving terminology and concepts from this document. "Access and Amendment" is essential in the understanding of the role of the person whose data is being taken. "Access and Amendment" ensures that individuals have not only the opportunity to access

[62] Ibid.

what information is being stored about them, but also to be able to correct incorrect the collected information on themselves. “Accountability” and “Transparency” help better inform conversations around the necessity of agencies to have oversight in the way in which they conduct activities related to PII. “Authority” again ensures that there are certain exclusive rights given to the individual whose data is being collected. “Minimization” will be key in understanding the philosophy behind many of the acts passed surrounding the collection of data. While it would greatly benefit the U.S. Federal Government to have access to as much information as they can collect, the FIPP ensures that there is a consideration and a check towards the decrease in collection. “Quality and Integrity” has to do with the “fairness” towards individuals on how their data represents them. This is to avoid situations in which a person could experience negative consequences if their data is incorrect (e.g. someone not being able to take out a loan because their credit score was incorrectly recorded). “Individual Participation” relates back to the idea of who has “control” over their own data. By allowing individual participation with a person’s data, they are ceding more control over to the person. “Purpose Specification and Use Limitation” goes hand in hand with the ideas of minimization. While not only should any given organization minimize the amount of data they collect, they should limit the ways in which they use this data. In also disclosing for what purposes the data is being used, the consumer can make a more informed decision when consenting. “Transparency” is the last principle, which is always important to include to keep accountability. Overall, many of these concepts will continue to be used in various forms throughout different laws in the United States, and throughout this thesis. Especially as it concerns data privacy or digital sovereignty, many of these various principles being violated is an indicator that there may be some sort of infringement on someone’s privacy or a nation’s sovereignty.

Efforts to expand this privacy framework to the digital came in 1986 with the *Electronic Communications Privacy Act*, which was originally intended to prohibit the unauthorized interception of wire, oral, or electronic communications.[63] While groundbreaking at the time it was passed, in 2024, it does not hold up to the standards that are necessary to properly safeguard U.S. citizens' privacy as it pertains to the digital landscape because of the fact that technology and constitutional law have come so far in this time. Aspects of the act, such as the differentiation between real-time and stored access, simply are not adequate in 2024 to address modern privacy challenges.[64] According to University of Pennsylvania law professor Orin Kerr, a modern version of the Communications Privacy Act would need to incorporate four main features.[65] Firstly, it should impose a uniform requirement for a warrant. Secondly, it should impose particularity requirements for what it calls "noncontent data" (data that does not directly pertain to the content of the piece of information, but rather could be a piece of surrounding information such as the time of a text message, rather than the content of the message itself). Thirdly, this 2024 law would apply minimization rules to all accessed content, and lastly have different provisions for U.S. and foreign users.[66] Ultimately, when it comes to U.S. online data protection, there are many ways in which the current legislation needs to be updated to best serve the needs of the American people.

---

[63] Electronic Communications Privacy Act of 1986, Public Law 508, U.S. Statutes at Large 100 (1986): 1848-1873. https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1848.
[64] Orin S. Kerr, "The next generation communications privacy act," *University of Pennsylvania law review* (2014): 373-419.
[65] Ibid
[66] Ibid.

Information Sharing and the Health Insurance Portability and Accountability Act

In 1996, one of the more famous acts of the ones being reviewed was passed, the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was critical in being the first national privacy protection for health information.[67] The most critical and relevant part of HIPAA was its "Privacy Rule," which established national standards, and was adopted in the year 2000 because Congress did not enact new privacy laws three years after the enactment of HIPAA.[68] This importantly outlines what is called "individually identifiable health information," which includes demographic details such as payment information or health conditions. While *de-identified* health information is essentially free use, individual identifiable health information was created as a concept to prevent an individual's information being disclosed to another entity without their permission.[69] Here, we can see the outlines of what eventually becomes part of major privacy laws across U.S. states. Essentially, HIPAA is one of the first pieces of legislation in the United States that allows the individual to have a say and control in what happens to their personal information. There are still exceptions to this, however, such as judicial and law enforcement being able to still have access to this individual identifiable health information under certain circumstances. In addition, HIPAA is quite limited in scope and can only protect U.S. citizens' health data and other data directly related to it.

---

[67] Office of the Federal Register, National Archives and Records Administration," Public Law 104 - 191 - Health Insurance Portability and Accountability Act of 1996," Government. U.S. Government Printing Office, August 20, 1996, https://www.govinfo.gov/app/details/PLAW-104publ191

[68] Ibid.

[69] Ibid.

Children's Protections

Right around the time, slightly after HIPAA was passed, another critical privacy act, the Children's Online Privacy Protection Act (COPPA), was adopted into law.[70] This act aims to protect the privacy of children under the age of 13 through the regulation of the collection, use, and disclosure of their personal information on the internet.[71] COPPA outlines several different regulations, all of which work towards this goal. Operators must provide notice of their information collection practices, allow the deletion of children's information at the request of their parental or guardian's consent, allow access to review, limit the data collection of children, and establish procedures to protect the confidentiality, security, and integrity of children's information online.[72] Much of the language used in this document are similar to that of the Fair Information Practice Principles (e.g. access, deletion, and limitation being explicitly part of this act), and in many ways this allows us to see that there are consistencies in the ways in which the United States federal government views how privacy can best be protected. Importantly also, there are provisions in this act that prevents the selling of information to third parties without the explicit consent of the parent or guardian.[73] However, as was the issue with HIPAA, COPPA is very limited in scope. While it is important to protect the privacy of children, it should not preclude the protection of the rest of the country as well.

While The Privacy Act of 1974, HIPAA, and COPPA are not necessarily the only laws that aim to protect the privacy of U.S. citizens but are some of the more essential to obtain a general understanding. Importantly, however, none of these acts are actually comprehensive

---

[70] CHILDREN'S ONLINE PRIVACY PROTECTION, U.S. Code 15 (2011), §§ 6501-6506, https://www.govinfo.gov/app/details/USCODE-2011-title15/USCODE-2011-title15-chap91.
[71] Ibid.
[72] Ibid.
[73] Ibid.

privacy protections for all U.S. citizens for all of their online data. Either limited in scope by type of data or through the legal applicability of the laws in practice, the U.S. lacks an act that protects *all* data for *all* of its citizens, despite having clear frameworks and examples of ways in which they have protected online information in the past. In addition to this, there are acts that many believe work against the protection of privacy of citizens in the United States.

The USA PATRIOT Act

In the wake of the attacks on September 11th, 2001, the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (the USA PATRIOT Act) was passed.[74] The USA PATRIOT Act was an attempt from the U.S. Federal Government to counteract future terrorist attacks like the ones seen on September 11th through preventive counterterrorist measures.[75] In the name of counterterrorism, the federal government seized the authority to access much more information than it otherwise would be able to prior to these attacks. Each sector with which the USA PATRIOT Act deals changes the way in which PII is viewed, as well as the dynamic of the handling and collection of these PIIs. Financial institutions, libraries, educational institutions, internet and communication companies, and transportation are all affected.[76]

To stop potential terrorists from being able to finance their attacks or organizations, the access of law enforcement and intelligence officials to financial records of individuals was

---

[74] U.S. Congress, House, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, HR 3162, 107th Cong., 1st sess., introduced in House October 23, 2001, https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162ih/pdf/BILLS-107hr3162ih.pdf

[75] Ibid.

[76] Priscilla M. Regan, "Old issues, new context: Privacy, information collection, and homeland security," Government Information Quarterly 21, no. 4 (2004): 481-497.

expanded. The Right to Financial Privacy Act of 1978 was amended under the USA PATRIOT Act to allow financial information and records to be disclosed.[77]

Libraries, according to section 215, allows the Federal Bureau of Investigation to request and obtain library records of library patrons without their knowledge or consent. This information can include anything from the reading habits to the internet usage of any given library user.

Educational institutions were also affected via the amendment of the General Education Provisions Act, which now allows the Attorney General or any designated federal officers to submit a written request to receive educational institutions to cede access to educational records, in the name of counterterrorism.[78]

Internet and communication companies and transportation operate in similar ways as the other institutions that have been affected by this act. Essentially, in the name of counter-terrorism, the United States federal government is able to access otherwise private information on anyone who uses a variety of U.S.-based institutions.[79]

The way in which the USA PATRIOT Act interacts with these varying institutions shows the government's massive reach into the lives of individuals in the name of national security and counterterrorism.

While according to the way in which the USA PATRIOT Act is written, it appears to be very limited in scope. If a person is not participating in terrorist activities or activities that could be suspect of terrorism, there allegedly should be nothing to worry about. However, in practice, this is a very risky act to the privacy of the hundreds of millions to whom this law applies.

---

[77] Ibid.
[78] Ibid.
[79] Ibid.

Terrorism, according to the USA PATRIOT Act, is defined to be any activity that involve acts dangerous to human life or that would violate any law of the United States.[80] In addition to this, terrorism is expanded to also mean any activity intended (which is legally very hard to prove) to intimidate or coerce a civilian population, influence the policy of the government through coercion or intimidation or affect the conduct of a government through mass destruction, assassination, or kidnapping.[81] While much of this is very clear-cut, such as kidnapping and assassination, "intent" to "intimidate or coerce" a civilian population and "influence" the government through these methods are a little more vague.[82]

Lastly, the United States in many ways could within its own legal limits use this act to infringe on the privacy of non-U.S. citizens or entities, as the operations only need to "primarily" occur within the territorial jurisdiction of the United States.[83]

The Foreign Intelligence Surveillance Act Post-USA PATRIOT Act

It is also important to note the implications of the amendments made to the Foreign Intelligence Surveillance Act (FISA), because of its controversial nature. FISA is has drawn much attention for many Americans because of the rights that it grants the U.S. Federal Government. While originally created to protect against the government surveillance of U.S. citizens, it has quickly become a way for the government to collect information on millions of U.S. citizens and foreign citizens alike.[84] When FISA was first passed in the United States, it was very limited in what investigators from the National Security Agency (NSA) and the Federal

---

[80] Ibid.
[81] Ibid.
[82] Ibid.
[83] Ibid.
[84] Paul T. Jaeger, John Carlo Bertot, and Charles R. McClure, "The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act," *Government Information Quarterly* 20, no. 3 (2003): 295-314.

Bureau of Investigation (FBI) could do.[85] The USA PATRIOT Act is notorious for expanding many of the powers of the government as it pertains to FISA, as it amends this act in the name of counter-terrorism. The PATRIOT Act fundamentally changes many of the aspects of FISA as it was originally seen when it was first passed in 1978. Some notable alterations made to this act because of the PATRIOT Act include the expansion of the definition of records, changes in the standards for investigations, and the increased sharing of information between agencies. While these seemingly don't seem to cause any alarm on their own, in aggregate they create an easier way for the government to collect and use data.[86]

Before the USA PATRIOT Act, there were very limited and specific records which could be obtained and used in FISA investigations (e.g. hotel registrations and storage unit rentals).[87] Under the post-PATRIOT Act FISA, "any tangible thing (including books, records, papers, documents, and other items)"[88] can be used in an investigation, which widely expands the authority to which FISA investigators have access.

There are many ways in which the standards for investigations changed under the USA PATRIOT Act's expansion of FISA. One of the most major points of contention is the fact that FISA investigations now will be able to be approved even if the purpose of it is not directly related to foreign intelligence, because after the amendments only a "significant" portion of the purpose of the investigation needs to be present.[89] While not necessarily used often, this does

---

[85] Delaney, Kellie. "The USA PATRIOT Act and Privacy: A New Frontier of Mass Surveillance." *GP Solo*, vol. 37, no. 5, 1 Sep. 2020, pp. 34 - 37.
[86] Ibid.
[87] Paul T. Jaeger, John Carlo Bertot, and Charles R. McClure, "The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act," 2003.
[88] United States. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 or FISA Amendments Act of 2008. [Bethesda, MD :ProQuest], 2011.
[89] Ibid.

create an area in which investigations can be opened for data collection, which wouldn't have necessarily been approved pre-USA PATRIOT Act FISA.[90] This expands the reach of the federal government to collect information, as well as expanding the amount of data that can be collected. In doing this, while not technically out of line with the FIPPs, the federal government expands its authority over what data it can collect and the amount of data collected becomes expanded, rather than minimized.

Since the USA PATRIOT Act, FISA has been revised multiple additional times. In 2008, the FISA Amendments Act expanded FISA to authorize unlimited acquisition of international communications and lifted restrictions that prevented the federal government from needing a named target to obtain a surveillance order.[91] This additionally further expands and maximizes the amount of data that the federal government can collect.

Homeland Security Act

In 2002, also in reaction to the attacks on September 11th, 2001, the Department of Homeland Security was tasked with various other responsibilities and key management issues. Much of this had to do with the coordinating and sharing of information related to threats of domestic terrorism.

The Homeland Security Act emphasizes the importance of the sharing of information between the private sector and the government, especially as it comes to critical infrastructure protection and cybersecurity. Importantly established when talking about the private sector's relationship with sharing information with the federal government, Information Sharing and

---

[90] Jaeger, Paul T., John Carlo Bertot, and Charles R. McClure. "The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act." *Government Information Quarterly* 20, no. 3 (2003): 295-314.
[91] Delaney, Kellie. "The USA PATRIOT Act and Privacy: A New Frontier of Mass Surveillance." *GP Solo*, vol. 37, no. 5, 1 Sep. 2020, pp. 34 - 37.

Analysis Centers (ISACs) were created. ISACs are entities that serve to gather, analyze, and disseminate information to and from infrastructural institutions and the federal government. ISACs are essentially organizations that exist to facilitate the exchange of information between the private sector and the federal government. The Homeland Security Act thus not only encourages but necessitates open communication and information sharing.

Social Media Corporations as Data Brokers

It is no surprise that large social media companies use user data in a variety of ways. Simply opening any social media application, it is clear to see through the advertisements and the specificity of the algorithms' feeds that social media platforms have multitudes of data saved on their active users. While the privacy policies vary across social media platform and across the country in which it is operating, a recent study found that social media networks exploit the weaknesses in the current legal frameworks in the United States to exploit the maximum amount of data.[92] In addition to this, social media platforms hide the ways in which they collect data from users and often fail to disclose the purposes for which they are collecting this personal data in the first place.[93] Through various predatory practices, such as contests or cookies, many of the largest social media platforms like Facebook, YouTube, and Twitter can collect massive amounts of data on its users, in the name of a "better" user experience.[94]

This becomes especially problematic when considered in the lens of the laws that allow the U.S. federal government to have access to much of this data through various counter-terrorism acts that have been passed. More essentially though, these are ultimately private

---

[92] Germán Llorca Abad, and Lorena Cano Orón, "How social networks and data brokers trade with private data," *Redes. com: revista de estudios para el desarrollo social de la comunicación* 14 (2016): 84-103.
[93] Ibid.
[94] Ibid.

corporations that have stored trillions of user interactions with their platforms. There is an unfathomable amount of data that private companies hold, without always necessarily having the proper methods for the safe storage of this data.

The Era of Big Data and Big Data Breaches

Data brokers have access to wide ranges of information on individuals, including, but not limited to, social security numbers, addresses, birth dates, and phone numbers. Much of this information is collected from public records (e.g. voter registration, driver's license information, etc.), and is then sold to private companies or the government generally to conduct background checks.[95] While not inherently unsafe in and of itself, the data brokerage industry does require massive amounts of information on people to be collected in order to conduct business and grow. Without proper regulation, data brokers are incentivized to collect as much data as possible on as many people as possible to turn a larger profit. This is true because of the origins of the industry and the way in which the industry makes profit. While some information that data brokers collect is subject to regulation, such as the collection of credit card information, much of what is collected is generally not regulated on a state or federal level.[96] There is also much criticism drawn with data brokers' close relationships with government agencies with whom they conduct business frequently. For example, the largest data broker, ChoicePoint, had multiple millions of dollars in contracts with the Department of Justice during the time of the massive 2005 data breach.[97] Overall, in the United States, private corporations simply have too much power to

---

[95] Gina Marie Stevens Brooks, Stevens and HeinOnline U.S. Congressional Documents Library, *Data Brokers: Background and Industry Overview (RS22137)*. 22137 ed. S.l.: s.n.
[96] Ibid.
[97] "In re: Choicepoint, EPIC, https://epic.org/documents/choicepoint-2/

collect massive amounts of data on its users. Not only do they make profit off of this, but they are also not incentivized to follow safe practices by any national law.

This first serious case in which the severity of the consequences of mass surveillance by data brokers came with ChoicePoint. While originally starting as a breach that seemed to only involve tens of thousands of California residents, within the year, there were an estimated 163,000 victims of fraudulent actors accessing consumer data.[98]

A little over ten years later, in September of 2016, Yahoo! had an even larger breach with farther reaching implications. In this breach, at least 500 million user accounts were accessed, with compromised information including names, email addresses, phone numbers, passwords, and dates of birth, among others.[99]

In the following five years, there are three major other times in which data privacy and data security came to the forefront of the U.S. mind. One of the times was in 2018 Facebook-Cambridge Analytica Scandal, while in 2019 there was the Equifax data breach settlements and then the 2021 Google antitrust case.

It is because of large data breaches like these that it is always necessary to consider the data security implications as well as the data privacy implications of laws and regulations. A critical aspect data privacy is the fact that only through consent can personal data be accessed, without proper data security measures, user data can be at risk to unauthorized entry. In addition to this, as there becomes an increasing amount of data being collected on social media users, it is

---

[98] Paul N. Otto Annie I. Anton and David L. Baumer, "The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information," *IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Secur. Privacy*, vol. 5, no. 5, 1 Sep. 2007, pp. 15 - 14.
[99] Weiss and HeinOnline U.S. Congressional Documents Library, *Yahoo Data Breach - Issues for Congress (IN10586)*. 10586 ed. S.l.: s.n.

inevitable that social media companies will have more data to be stored. The risks to data privacy of hundreds of millions have only become larger over the years.

Conclusion

As we move into the future, there are many critical aspects of the way in which the data privacy policies operate that need to change in order to best protect U.S. citizens' data. The current policies set in place in the United States are simply not adequate in the proper handling of U.S. user data. While some current federal policies like HIPAA and COPPA delineate some specific situations in which privacy is to be properly handled, there are also acts like the USA PATRIOT Act which seeks to expand the powers of the federal government to infringe on privacy. Looking at HIPAA and COPPA, we can see areas in which the U.S. Federal Government has already created a lens through which it views privacy, all that needs to happen now is for it to get implemented on a national scale. To see how policies like these look on a state level in the United States, the following chapter is a case study on the Commonwealth of Virginia.

Chapter 2: Virginia is for Data Privacy Lovers

Introduction

The following chapter is a case study into the real-world application of data security and privacy protection landscapes in the context of the United States in the 21st century. Virginia has been one of the most proactive states in protecting its citizens' data privacy and security in a myriad of different capacities. To better explore the topics surrounding what happens to consumer data in the Commonwealth of Virginia, it is essential to identify key pieces of legislation which work towards a comprehensive data environment. This chapter looks into two different phenomena in Virginia, data privacy and its implications for digital sovereignty.

The purpose of the first part of this chapter is to look at how privacy apparatuses are already operating in the United States at a smaller, but still large, level. By looking at this, we can see the successes and drawbacks of implementing privacy laws in a United States cultural environment. While not necessarily a direct microcosm of the United States, Virginia was chosen because of its demographic similarities to the nation as a whole, including but not limited to some factors including its political, ethnic, urban/rural, and age diversity.

Ultimately, data privacy laws like the ones found in the Commonwealth of Virginia can be very beneficial to the consumer, yet also cause their own problems when dealing with the institutions they are regulating. Educational institutions and small businesses are two sectors of any state that are encouraged to grow because of their positive knock-on effects like higher educational attainment and impacts on local communities. Data privacy laws like the ones explored below are at risk of inhibiting the full functioning of institutions such as these. To further explore these claims, an autoethnographic study was done into running a small business

that has to come into compliance with Virginia laws, as well as a study at my institution, the University of Virginia.

The chapter is structured to answer the questions of what data privacy and security laws currently are, as of 2024, as well as how these laws affect not only consumers, but also institutions in Virginia, such as small businesses and universities. The most critical piece of recent legislation that has been passed in Virginia that will be explored in depth is called the Virginia Consumer Data Protection Act, henceforth referred to as the CDPA. Similar in nature to the European Union's General Data Protection Regulation and California's Consumer Privacy Act, the CDPA's goal is to create a comprehensive privacy protection and management structure in the Commonwealth of Virginia. In order to better understand this, the privacy landscape of Virginia is evaluated leading up to the 2023 passage of the CDPA, highlighting important acts that shape this.

In addition to the CDPA, the Governor of Virginia, Glenn Youngkin announced an executive order after the passage of the CDPA whose aim was to further protect the data privacy of Virginians against foreign threats, namely the Communist Party of the People's Republic of China.[100] While important to consider national security concerns at a state level, there are still far reaching ramifications. In addition to this, Chapter 768 passed in the 2023 session of the General Assembly of Virginia amended and added sections which dealt with state government electronic information.[101] In addition to the creation of additional cybersecurity provisions, the act also puts

---

[100] Office of the Governor of the Commonwealth of Virginia, *BANNING THE USE OF CERTAIN APPLICATIONS AND WEBSITES ON STATE GOVERNMENT TECHNOLOGY* by Glenn Youngkin. (Richmond, Virginia, 2022).
[101] Virginia Congress, *Chapter 768*, 2023 session, https://lis.virginia.gov/cgi-bin/legp604.exe?231+ful+CHAP0768

into law the prohibition of employees or government agents from downloading or using applications like TikTok, WeChat, or other specific applications developed by ByteDance and Tencent Holdings.[102]

While the future of data privacy and security might not be focused on the Commonwealth of Virginia, it is important to see how local governments are responding to international trends. Data protection begins at a small level. Overall, this chapter intends to inform what a national privacy legislation could look like, and what the functioning of it looks like in a U.S. state.

Ye Olde History of Virginian Data

Laws passed in Virginia that pertain to data privacy and protection have been taking form in many ways on a similar timeline to the United States as a whole. By exploring the history of Virginian data laws, we can see how on a smaller scale, state governments are trying to implement their own forms of data protection. By looking at these laws, we can see that there is precedent for a uniquely American view and application of data privacy. While laws passed in Virginia may not necessarily be the best for the United States on a national level, local and state laws are still important in their abilities to test legislation at a small level. As we will see as this chapter progresses, while there are various acts in Virginia aimed at protecting consumer data privacy, many of these laws still come at a cost. Ultimately, we are brought back to a question that was posed in the introduction, which is: to what extent should people's personal data be given away for the proper functioning of a society?

In the 2011 session of the Virginia legislature passed the Personal Information Privacy Act (henceforth referred to as VPIPA). This act was aimed to better regulate the collection and

[102] Ibid.

use of personal information by local and state governments in Virginia.[103] In many ways, there are ways in which this lays the groundwork for the CDPA, much of the language used is similar, and many of the rights afforded to the citizens by the Commonwealth of Virginia are similar to those that will be discussed further on in this paper. Some of the provisions that are discussed and ensured under VPIPA relate to data transparency, data security, and the rights of individuals as it relates to their relationship with their own data.[104] There are several sections found throughout that are aimed to protect Virginians. However, it is also important to note the places in which this piece of legislation still lacked.

Looking at section 59.1-442, there is a specific prohibition of merchants in Virginia from selling information to a third party that is gathered by customers during the sale, rental, or exchange of "tangible" personal property, without the explicit notice of this to the purchaser.[105] In addition to this, the section prohibits the sale of information gathered through various methods, such as personal checks, credit cards, or through driver's license numbers.[106] The main issues with this section as it translates to the climate of data collection and privacy in 2024 is that it first is mainly referring to the regulation of information collection at a very limited scope. Not only does this only refer to the exchange of the tangible, but it also limits the specific and limited types of transactions that are protected. The following section also outlines various exceptions to the already limited rules.

---

[103] *Personal Information Privacy Act*, Code of Virginia, 2011, https://law.lis.virginia.gov/vacodepopularnames/personal-information-privacy-act/
[104] Ibid.
[105] Ibid.
[106] Ibid.

The following three sections operate in a similar way to section 59.1-442, but just emphasize other specific situations in which consumer data is protected. Section 59.1-443.2 talks about social security numbers, while the following section talks more about driver's license protections.[107] The last section is interesting to note, however, as it outlines a legal recourse for individuals who have been victims of violations of VPIPA.[108] Overall, however there are many clear ways in which the scope of this act is limited in nature, and does not translate well to the digital world. It is foundational in safeguarding individuals' personal information from unauthorized sale, recording, and dissemination in the Commonwealth of Virginia. It also is important to emphasize that this was at the early stages of conversations around consumer data protection.

Five years later, in 2016, the Virginia legislature passed the Electronic Communications Privacy Act (VECPA), which the goal of governing the interception, access, and disclosure of electronic communications.[109] This legislation essential in the transferring of privacy legislation from a mostly physical realm to that of the electronic. Emails, text messages, and other forms of digital communication became protected in some way. Essentially, this act introduced regulations for agencies' access to electronic communications.[110] Under this, there was also the establishment of the procedures for obtaining warrants and court orders.[111] There was a focus on

---

[107] Ibid.
[108] Ibid.
[109] *Electronic Communications Privacy Act*, Code of Virginia, 2016, https://lis.virginia.gov/cgi-bin/legp604.exe?171+sum+SB599
[110] Ibid.
[111] Ibid.

data privacy and security in this law through regulation of the obtaining and storage of information.[112]

Overall, like the United States federally stands today, there was a time during which the Commonwealth of Virginia experienced its own issues and gaps in data privacy policies. However, as we will see in the following section, there are ways in which the gaps can be filled in order to best protect the data of all citizens.

Virginia Consumer Data Protection Act (CDPA)

In 2021, the Commonwealth of Virginia became the second state in the Union to pass a comprehensive consumer data protection act, aptly entitled the Consumer Data Protection Act, which aims to regulate the processing and protection of personal consumer information.[113] It mainly does this through the definition of consumer rights, such as the right to access, correct, delete, and obtain a copy of their personal data.[114] In addition to these rights, there is also a right to opt out of targeted advertising from companies, as well as to opt out of the sale of personal data.[115] On the data security end, the act outlines the responsibilities of data controllers, which includes safe practices, limiting of collection to only necessary information, and non-discrimination provisions for consumers who are trying to exercise their rights.[116] Even more than just this, the act also requires controllers to provide a clear privacy notice to their consumers, which discloses the way in which the personal data will be processed for targeted

---

[112] Ibid.
[113] *Chapter 53. Consumer Data Protection Act,* Code of Virginia, 2021, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/
[114] Ibid.
[115] Ibid.
[116] Ibid.

advertising.[117] Notices must also include the means by which consumers can exercise their rights under this act, which helps Virginians make informed decisions about their data and understand how it is being used.[118] This act offers many important protections for consumers which are essential to the preservation of their rights. Overall, this act is the piece of legislation, I argue, that would best be suited to handle some of the gaps that we see in privacy policy today in the United States on a federal level.

The right to access personal data allows the individual whose data is being collected to understand how their personal information is being used, and what is being stored about them. Through the empowerment of knowledge, consumers can now verify the accuracy of the information held about them.

In order for the right to access data to be of most use for consumers, correction is another essential right in ensuring the enduring accuracy and completeness of the information that is held by the business or organization. There are many consequences for outdated, inaccurate, or incomplete data being held by businesses, which can affect many facets of their lives. Some consequences can include negative ramifications for consumers their access to certain services, opportunities, and rights. The right to correct this information allows individuals to rectify the integrity of their records.

Going hand-in-hand with correction comes deletion. This is famously referred to as "the right to be forgotten" in many contexts. In addition to simply being able to update or change information, the CDPA also allows individuals to delete their personal information from the

[117] Ibid.
[118] Ibid.

systems and databases of businesses and organizations, for example when the data collected is no longer necessary, or if the data had been unlawfully processed. Consent to an individuals data can also be spontaneously retracted.

In order to do all of this, it is essential that consumers are able to obtain a copy of their records, which promotes transparency and accountability. Without this, access, editing, and deleting data would not be possible. By obtaining a copy, consumers can better understand and verify the accuracy of their information, which in turn assists them in exercising their rights under this law.

In addition to the protections that are given to consumers, on the other end, these protections enhance transparency by businesses and organizations. Through the necessity of the disclosure and say that consumers now have in relation to their personal data, businesses are forced into compliance through individuals. This also in turn can incentivize businesses to adopt responsible data practices and prioritize the protection of consumer privacy. In addition to this, businesses are charged with data minimization and purpose limitation clauses. These clauses encourage businesses to collect and store only the consumer information that is strictly necessary for the purposes for which they were collected, which must be limited in scope.

Data security is also enhanced under this act, which requires businesses and organizations to implement data security measures which protect consumers' personal data from unauthorized access, disclosure, alteration, and destruction.[119] These measures are intended to mitigate against

[119] Ibid.

the risk of widespread data breaches. Lastly, consumers under this act have the right to redress mechanisms.

Overall, there are many ways in which acts like the CDPA can increase the protection of rights of the everyday consumer. This is a major piece of legislation that attempts to fill the gaps on a state level, what should be done on a federal level. The diction used in the CDPA shows that there is a specific way in which we can talk about data privacy on a federal level. However, it is also important to consider the possible cons of new pieces of legislation. One possible drawback is that new compliance materials can be difficult on small businesses, especially those with limited fiscal resources or those who don't have much time. The following section aims to explore the extent to which there is an effect on small businesses.

The Impact on Small Businesses

Small businesses are thus being explored not only because of their importance to the functioning of the U.S. economy and society, but also because they are the ones who are going to be most affected by laws implemented with the goals of protecting data privacy. Larger businesses generally have legal teams who are paid full-time to decipher and put the company into compliance with these laws. Smaller businesses generally have less funds and often lack legal teams who can deal with the ever-changing legal landscape. In order to keep in compliance, small businesses are often forced to strain their already limited time and sometimes money.

To best understand the difficulties that additional compliance laws have on small businesses, I conducted an auto-ethnography on my process of creating a privacy policy document that would be in line with Virginia's laws, using my own small business as a case

study. I did this in order to best understand exactly what impact, if any, this law can have on already money-tight businesses across the Commonwealth of Virginia.

Starting off my journey into CDPA compliance, I simply researched online the quickest and easiest way to create a privacy policy document. I was sure to go out of my way to look for services that were free online and readily accessible. Ultimately, I decided to use a free online resource that is specially designed to create privacy policies that are compliant in the Commonwealth of Virginia, while also being able to select compliance goals from other places as well, including California, the E.U., and Canada. The website used for the purposes of this study is Termly, which is marketed as an "All-In-One Compliance Solution for Small Businesses." I chose to use this website over others simply because it showed up first on the Google search results, looked the most legitimate, and the marketing/aesthetics of their advertising and page layout.

Termly asks the user, presumably the owner or some form of legal council for a small business, a variety of questions which relate to the situation of the small business and its data collection policies. It is set up as a questionnaire, and is put in accessible English. The entire process took me about 45 minutes, and after it was completed, the service ended up actually being free of charge, as long as it is considered free to create an account with an email address. The other limitation for free users was the limited downloading options, which ultimately led me to other issues, such as figuring out how to insert HTML code into my website. The amount of time it took to complete included the time in finding an appropriate and trustworthy website to use, creating an account, taking the questionnaire, and uploading the document to my website. A few questions required me to consult the website builder I was using, as well as Google Analytics, which I use for my business, to see what data they collect on users of my website.

Questions ranged in focus, with some asking about target demographics of users (e.g. age, location, education status, etc.), others were more focused on the data that would be collected by the website, app, or otherwise (e.g. biometric, financial, social security, etc.). All questions included an explanation of what exactly was meant by the question, a function which I used on the majority of my questions when responding. There was also a digital chatbot should the Termly user need additional information. The chatbot was manually run by employees at Termly.

Overall, I found that the process of creating a CDPA-compliant privacy policy is not the most difficult, and can be done with simple access to the internet and an email address, which most small businesses who are operating websites that collect users' data should already have. While it did take some time, it was not significant enough to hinder any business. It is also important to note that this process is only required of small businesses in Virginia who collect the data on more than 100,000 unique consumers. If a business is operating at this large of a level, it is unlikely that compliance measures would be a serious hindrance.

Overall, this is essential in understanding how laws enacted in Virginia can affect many facets of a society, even when there are the best intentions. I found that the argument that a policy such as this could harm small businesses is not necessarily founded, as there is little required in order to best protect the safety of consumers.

Virginia Versus ByteDance and Tencent

Virginia governor Glenn Youngkin passed his 24th executive order in 2022, whose primary purpose was to ban the use of Chinese-owned TikTok and WeChat on state government technology (or any other application that is owned or developed by ByteDance Limited or

Tencent Holdings Limited).[120] Youngkin argues that there is a large significance that needs to be placed on the safeguarding and ensuring of cybersecurity within the state government, and banning TikTok and WeChat is the best method for protecting sensitive data, such as healthcare and tax information, from being breached to any foreign power, namely the Chinese Communist Party's government.[121] Other than for public safety purposes, this order prohibits the use of either of these apps, or the visitation of their websites, on *any* government-issued device (whether leased or state-owned), unless there is a public safety concern which requires the appropriate authorities to use TikTok or WeChat.[122] In addition to devices, access to ByteDance Limited or Tencent Holdings Limited is prohibited on Commonwealth-owned, operated, or maintained wireless networks.[123]

This order addresses the need of the state government to safeguard sensitive data and ensure that there are proper cybersecurity measures in place.[124] If nothing else, this act serves as a statement and an example for what the Commonwealth of Virginia believes is necessary to protect its digital sovereignty. This is also in line with the Department of Defense's similar measures to remove TikTok, WeChat, and other similar applications and websites from federal government-issued devices and wireless networks. After this was enacted, within a year, chapter 768 was passed, which overrides the executive order.[125]

---

[120] *BANNING THE USE OF CERTAIN APPLICATIONS AND WEBSITES ON STATE GOVERNMENT TECHNOLOGY*, Glenn Youngkin. (Richmond, Virginia, 2022).
[121] Ibid.
[122] Ibid.
[123] Ibid.
[124] Ibid.
[125] Ibid.

The concept of a "TikTok ban" is critical to evaluate at the state level for a few reasons. On the one hand, we can see the practical effects that this has on a variety of institutions, such as educational institutions, who must comply with regulations. When scaling this to a national level, it is important to see how various facets of society are affected. In addition to this, it is important to see whether a ban is the most effective way of accomplishing a goal. While the government of the Commonwealth Virginia doesn't quite have the power to force a sale of TikTok to a non-Chinese owned company, a ban isn't necessarily the only option to protect data security for the everyday Virginian. Some possible alternatives that Virginia could have taken is the force of data localization for Virginians' data, further transparency on what exactly is happening to data, data access restrictions on data that TikTok can collect, or even the encouragement of TikTok's competitors to naturally subdue its influence.

Cons of a "TikTok Ban"

While ultimately this executive order and the following laws were passed with the best of intentions for the safety and well-being of the Commonwealth as a whole, there are still many implications that need to be taken into consideration when evaluating the effectiveness. For employees of and entities who are contracting technology with the Commonwealth of Virginia, there are serious implications on technology usage. In terms of communication with large audiences, TikTok and WeChat both provide essential services to millions. Especially when it comes to international communication with the People's Republic of China, many individuals and organizations may have come into some major difficulties. In addition to this, while still a state and not yet on the federal level, there are many implications of potential ramifications by the Chinese government on what is a seemingly political move against the Chinese Communist Party and their practices.

One of the most important things to consider with this, however, are the challenges in enforcing monitoring compliance with the order, especially in ensuring that all government-issued devices and wireless networks are free of the prohibited applications and websites.

Effects on Public Universities in Virginia

This paper was written in the Spring of 2024 at the public institution, the University of Virginia, during which time chapter 768 of the Virginia code was still in effect. At the time of the research being done at the time, the University of Virginia was *not* in compliance with this act for two reasons. In addition to being able to access TikTok and WeChat from U.Va.-operated wireless network, *eduroam*, these websites were also available to use at full functionality on public, U.Va.-owned computers in the public libraries. On an operational level, it is understandable why the university is not in compliance, as it is timely and possibly expensive to change all wireless networks and computers from accessing a myriad of websites.

Because of this, there is a natural conflict between the University and the Commonwealth. While the Commonwealth is mandating complete erasure of Chinese-owned applications and websites, the University of Virginia believes that it is still fully in compliance with Virginia law. Complications arise with the concepts of banning large applications like TikTok when freedom of speech is involved, which is protected and promoted at the University of Virginia. According to the National Constitution Center, when a federal district court judge was faced with a TikTok ban, the judge “was presented with several First Amendment arguments. TikTok believed that the ban restricted free speech and failed under strict scrutiny, a test that requires the government to show a compelling interest that is narrowly tailored in the

least-restrictive manner."[126] In this particular ruling, which pertained to the State of Montana's TikTok ban, freedom of speech was found to have been violated. The issue is to understand to what extent the issue of TikTok is a matter of free speech, as it has come to be considered by many as a form of critical infrastructure.[127]

This ban on TikTok and WeChat, however, has many implications for students, faculty, and staff across the university community. People affiliated with the University from the People's Republic of China often use applications like WeChat to communicate with their friends and family back at home and abroad. By restricting access to applications and websites like WeChat, many international students are left with limited other communication methods. The University of Virginia essentially has become cut off from many major forms of communication with the second most populous country in the world.

In terms of its implications on other students and professors, the ban on these applications and websites can inhibit learning. While TikTok, WeChat, and others may pose some threats, there is a merit to learning about them. The simple fact that over 150 million Americans, and hundreds of millions of others worldwide, use these applications and websites can be grounds for it to be considered a critical communications infrastructure for many. Studying the world without limitations is one of the essential qualities that a public university must possess in order to be truly a comprehensive education. Because of the fact that these websites are now unable to be

---

[126] Scott Bomboy, "TikTok ban and the First Amendment," *National Constitution Center,* March 22nd, 2024, https://constitutioncenter.org/blog/a-national-tiktok-ban-and-the-first-amendment#:~:text=The%20judge%20was%20presented%20with,in%20the%20least%2Drestrictive%20manner.

[127] Zongyi Zhang, "Infrastructuralization of Tik Tok: Transformation, power relationships, and platformization of video entertainment in China," *Media, Culture & Society* 43, no. 2 (2021): 219-236.

studied while on the University of Virginia's campus WiFi, professors are forced into teaching materials that may not be as relevant, or may have to use party sources to access first-hand information from these websites.

While there is always a need to consider the safety of the university community first and foremost, there is also a necessity to consider what is best for the furthering of a holistic education for everyone, regardless of national origin. In the banning of major Chinese websites and applications, the Youngkin administration has isolated thousands of university students, and inhibited the learning of many more. Ultimately, there are many reasons for why a ban of Chinese-owned applications and websites would be a good and easy solution. However, a ban is not the most effective way of protecting the data privacy of Virginia residents, as many people and institutions are left with the tough decision on how to realistically integrate this into the everyday. Should a TikTok ban be passed on a federal level, many of these issues of restricting free speech, isolation of Chinese Americans, and loss of a competitive edge[128] will only be exacerbated when applied to hundreds of millions more people.

The University of Virginia has many issues to which it needs to respond. As the leading university in the Commonwealth, it is essential that U.Va. stands strong against administrations that aim to use politics to undermine the learning and interconnectedness of students.

Looking Beyond the Commonwealth

Future challenges include the banning of TikTok statewide, or even as of 2024 there are talks of national bans. While it is unclear what these bans might entail, there are already many

[128] Sabrina Moreno and Karri Peifer, "TikTok's economic impact on Virginia," April 8th, 2024, https://www.axios.com/local/richmond/2024/04/08/tiktok-s-economic-impact-on-virginia

debates surrounding the prospect. While an outright ban seems unlikely because of the inhibition of freedom of speech, thus violating the first amendment, there are other ways in which the United States Federal Government is trying to deal with this national security issue. One of the most likely courses of action is the forced sale of TikTok from its Beijing-based owner company. However, there are various domestic and international implications for this as well.

As of April of 2024, the U.S. House of Representatives passed a bill entitled "Protecting Americans from Foreign Adversary Controlled Applications Act," whose main purpose was to ban TikTok on a national level.[129] The language used in the bill is quite harsh, indirectly referring to the People's Republic of China as a foreign adversary.[130] While it is impossible to predict whether or not this piece of legislation will be passed into law, there are still many implications surrounding the bill being passed in the House. For one, the vote to pass this in the House was 352-65, showing that there is widespread bipartisan support for the banning of TikTok, should it continue to be owned by an adversary nation.[131] This act specifically outlines provisions for the sale of applications or websites owned by the Chinese government, which essentially leaves the door open for TikTok to be sold by ByteDance to a company based in the United States, or possibly elsewhere.[132] A forced divestiture of TikTok would be an interesting solution, as it neither isolates anyone nor violates freedom of speech.

The following chapter will further explore the TikTok debate on the national level. While we have now seen the practical implications of an outright ban on TikTok for government

---

[129] U.S. Congress, House, Protecting Americans from Foreign Adversary Controlled Applications Act. H.R. 7521. 118th Cong., 2nd sess., Engrossed in House March 13, 2024. https://www.govinfo.gov/app/details/BILLS-118hr7521eh.
[130] Ibid.
[131] Ibid.
[132] Ibid.

employees and agencies on a state level, we can begin to better understand what possible bans would look like when applied to a much larger scale. Ultimately, we will explore how the application that was made famous by teenagers dancing has become a national security threat.

Chapter 3: The Decade of the Data-Hoarding Dragon

Introduction

This final chapter attempts to enlarge the scope of the previous chapter to see what some of the larger trends are on an international level between the United States and the People's Republic of China, specifically looking at TikTok as a friction point between the two countries. In order to best understand how TikTok has come into the precarious position in which it finds itself today, it is essential to first understand the current landscape of digital sovereignty.

This chapter will be organized around the "TikTok hearing" in March of 2023, officially known as "TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms."[133] In this chapter, I will conduct a textual and comparative analysis to analyze the rhetoric from the Chinese Foreign Ministry, the United States Congress, and from TikTok itself directly before, during, and after the hearing. The goal of this is to better understand the varying perspectives of three of the largest stakeholders in this geopolitical situation on a macro level.

---

[133] *TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms*. House of Representatives Energy and Commerce Committee, 2023. https://www.c-span.org/video/?526609-1/tiktok-ceo-testifies-house-energy-commerce-committee-hearing.

After an analysis of the testimony given by TikTok CEO, Shou Chew to better understand some of the policies and concerns that are being addressed by TikTok in response to the United States Congress. Alongside this, the privacy policy of TikTok and surrounding documents will be analyzed to see if it is in compliance with both U.S. policies and what it claims to be doing under their newest mission, Project Texas. After this, an analysis of the point of view of the Democratic Committee on Commerce and Energy will be conducted alongside that of Shou Chew. Lastly, responses given in the days following the TikTok hearing in March of 2023 by the Chinese Foreign Ministry in the United States will be explored. Overall, a comprehensive analysis of the various stakeholders and their perspectives will be collected through the lens of the TikTok "problem."

This all comes together to better inform what data privacy means when it comes to having multiple varying state actors involved. While it is one thing to have a domestic corporation collecting data on citizens, it is entirely different when other countries, especially foreign adversaries, have access to this collected data. Thus, this chapter expands on the ideas of domestic data privacy into the realm of how international data privacy plays into the concepts of digital sovereignty.

Digital Sovereignty

Like many concepts, digital sovereignty has an ever changing definition and cannot be easily defined well. Depending on the context, such as the country who is striving for this concept, digital sovereignty can refer a myriad of factors. It is important to understand that this is such a complex issue because this is central to much of the People Republic of China's and the United States' foreign policy as it relates to their digital realm. A journal article by Patrik Hummel, Matthias Braun, Max Tretter and Peter Dabrock perfectly explains the complexity of

digital sovereignty. After a review of 341 publications, the authors reveal that there is a diverse range of understandings of, and often a lack of clarity about, digital sovereignty.[134] There are thus, a varying amount of factors that play into the general idea of digital sovereignty, such as notions of control, ownership, and claims to data.[135] Digital sovereignty exists across a variety of different capacities, such as through legislation passed by governing bodies and through the physical existence technical facilities. Digital sovereignty is linked to the exclusive right of a nation to control what happens to own data. A couple of essential parts of digital sovereignty are similar to that of the ways in which an individuals are in control of their own data. The right of a nation to determine the use and dissemination of its data and data of its citizens is critical in digital sovereignty, which often is expressed through legislation that places more physical and legal control over various data.[136] In many ways, digital sovereignty operates in a similar way to data privacy, just on a larger scale between nation states. Issues such as access and deletion are two focal points of the concepts of digital sovereignty, but instead of an individual's data being protected and controlled from a larger institution or enterprise, a nation's data is being protected and controlled by another.

In terms of the following chapter, it is essential to understand the many facets of digital sovereignty because of the fact that this is a major reason for why TikTok has found itself in the position it is in now. While TikTok started as a seemingly harmless social media platform, it has transformed into a massive hoarder of U.S. data. In order for the United States to be able to exercise its complete control over its citizens' data, TikTok needs to be able to be controlled, to a

---

[134] Hummel, Patrik, Matthias Braun, Max Tretter, and Peter Dabrock. "Data sovereignty: A review." *Big Data & Society* 8, no. 1 (2021): 2053951720982012.
[135] Ibid.
[136] Ibid.

certain extent. By this, I intend to say that TikTok has become too large to be simply ignored by national governments, especially if allegations that it is ceding information to the government of the People's Republic of China without consent of the countries from where the information originates are true.[137]

TikTok's Data Privacy

Shou Chew is the CEO of TikTok since 2021, coming to the helms of the multinational corporation to steer it towards a more international platform.[138] Because of his standing as the CEO of TikTok, Shou Chew was called to testify in front of the United States Congress. The following section explores the CEO's written statement of testimony to best explore what the position of TikTok is as it relates to the issue of digital sovereignty. While TikTok is not the only social media platform to collect data on its users, it is the only one owned by a foreign adversary, and it is the fastest growing social media application in the U.S., which is why they were called to testify.[139] When pursuing digital sovereignty in any given nation, it is important to consider the fact that private corporations can be just as much of a threat, if not even larger of one, than other state actors because of the fact that there is less control over their actions. It is important to hear the perspectives of TikTok because of the fact that they have become a focal point in the issue of the digital sovereignty war between the United States and the P.R.C..

The TikTok CEO's written statement of testimony is a relatively short document, just 10 pages in length, which addresses many of the issues brought forth towards TikTok. It is

---

[137] Brian Fung, "Analysis: There is now some public evidence that China viewed TikTok data," *CNN*, June 8th, 2023, https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html

[138] Lauf, Florian, Simon Scheider, Jan Bartsch, Philipp Herrmann, Marija Radic, Marcel Rebbert, André T. Nemat et al. "Linking data sovereignty and data economy: arising areas of tension." (2022).

[139] Katharina Buchholz, "The Rapid Rise of TikTok," *statista*, October 7th, 2022, https://www.statista.com/chart/28412/social-media-users-by-network-amo/

organized with seven sections, plus an introduction section, entitled: TikTok's Commitment to Transparency, Minor Safety, Data Privacy, Keeping TikTok Safe for All, Data Security, Myths Versus Reality, and Conclusion. For the purposes of this section, the "Minor Safety" and "Keeping TikTok Safe for All" will not be analyzed, as they do not have to do with data security or digital sovereignty.[140]

The introduction section is full of positive remarks about TikTok, with it being described as inspiring creativity, helping small businesses thrive, and enriching people's lives.[141] This is a way in which TikTok has officially reacted to much of the flack that it's received from foreign governments, posing itself as not a threat to security, but rather an enriching experience for all who use it. Examples are used throughout to emphasize the great things that TikTok does specifically for the United States. Other than name-dropping a small business in Mississippi who was helped by TikTok, Chew states that TikTok is actually "a lens through which the rest of the world can experience American culture."[142] In doing this, Chew intends to underscore TikTok's importance not only as critical for the success and well-being of many Americans, but also is essential for the soft power of the United States. Essentially, Chew argues that both on a personal and national level, TikTok is a critical and helpful piece of infrastructure. He also makes it seem that TikTok is not just an arm of soft power for the People's Republic of China, but rather more beneficial to the United States. It is also important to note here that Chew separates himself from the People's Republic of China, stating that he is a third-generation Singaporean, educated in the

---

[140] Shou Chew, "Testimony Before the U.S. House Committee on Energy and Commerce Written Statement of Testimony; Testimony of Shou Chew Chief Executive Officer, TikTok Inc.," March 23rd, 2023, https://docs.house.gov/meetings/IF/IF00/20230323/115519/HHRG-118-IF00-Wstate-ChewS-20230323.pdf

[141] Ibid.

[142] Ibid.

United States and the United Kingdom, and served in the Singapore Armed Forces.[143] In the final remarks of the testimony, Chew addresses the concerns of members of the Congressional Committee, which he believes falls into four categories: minor safety, data privacy and security, real-world harms from online activities, and foreign content manipulation.[144] Importantly, the only non-section-header bolded words in the whole text are found in the introduction, which are the commitments that Chew makes to the readers. These commitments are safety (particularly for teenagers), protection of U.S. user data from foreign access, freedom of expression from manipulation from any government ("any" here is italicized, possibly referencing possible U.S. influence), and transparency to third parties to hold them accountable for their commitments.[145] For the purposes of the better understanding of TikTok within a digital sovereignty debacle between the United States and the People's Republic of China, the latter three commitments are the most important to explore. Protection from foreign access is one way in which Chew plays to the idea that TikTok will preserve the data sovereignty of the United States, preventing any nation from being able to obtain U.S. user data. This is followed by the freedom of manipulation, which Chew strategically states to ensure that the United States should not be worried about this being a form of soft power from the Chinese government. Lastly, by offering transparency, he checks of two boxes on some of the essentials of data privacy.

The section entitled "Data Privacy" is essentially split into two different ideas. The first part of this section talks about the intrinsic privacy properties of TikTok, exploring some of the privacy options that TikTok offers and the limited data it collects. The second part talks about the mistakes that TikTok has made, such as the TikTok meeting leak, which Chew condemns "in

[143] Ibid.
[144] Ibid.
[145] Ibid.

the strongest possible terms." He expresses how there will be consequences, remediation, and strengthening of policies around employee misconduct as it pertains to data privacy. Data privacy is a critical part of digital sovereignty, as if there are stringent data privacy regulations in place, there is no reason for why data can be exploited by any other entity.

Looking at this section through the lens of the CDPA and its affordances to Virginian consumers, data privacy does not seem to be as "critical" to TikTok's mission as Chew leads the readers to believe. While Chew addresses some of the needs of a company to protect consumer privacy, such as limiting the amount of data collected and transparency,[146] he does not properly address some of the critical components of consumer data privacy protection. While Chew explains that users have access to a "wide range of privacy settings,"[147] all of these have to do with specific TikTok application features, such as options for who can interact with users' videos or picking who can tag a user in a post. Access, correction, deletion, and obtaining a copy of a users' personal data are not mentioned. In this sense, Chew fails to properly address the complete range of what data privacy often entails when viewed through the lens of some of the United States' state's legislation.

The "Data Security" section delineates the main counter that TikTok has against claims of foreign powers being able to access or manipulate U.S. user data or experiences. This centerpiece project that TikTok has been working on is called "Project Texas."[148] This project, which as of the time of the writing of this thesis has not yet been given a release date, is wide in scope. In what Chew describes as an "unprecedented initiative,"[149] Project Texas is a package

[146] Ibid.
[147] Ibid.
[148] Ibid.
[149] Ibid.

that involves independent oversight to regulate TikTok from unauthorized access to protected U.S. user data and TikTok systems. At the time of the Congressional hearing, $1.5 billion had been invested on implementation of this, with a special-purpose subsidiary, TikTok U.S. Data Security Inc. also being founded.[150] Through this mission, TikTok is ensuring that data will be stored on American soil, with which U.S.-based Oracle will be charged.[151] Within a year, all U.S. user data obtained by TikTok will be stored in the United States using Oracle, with past data not stored through this method being deleted.[152] Chew seems to intend to use Project Texas as a way to fix the qualms of digital sovereignty that the U.S. government has, by taking foreign data and keeping it within the domestic realm.

For the first time on page 8 out of the 10 page testimony is the People's Republic of China mentioned.[153] This is critical to note because a lot of what the CEO of TikTok is trying to do is separate itself from the perceived influence that Beijing has on it.

Overall, it is important to look at these critical steps that are being taken to ensure data security, privacy, and sovereignty. The following section takes a deeper dive into TikTok's privacy policy and surrounding documents to better understand the practical applications of what Shou Chew is positing in his testimony. By looking at these documents, we can better understand the specifics of how TikTok is interacting with its user data in the United States. Their privacy policy is intended to be read by and applied to the everyday user, therefore it should be the most comprehensive legal document as it relates to these issues.

---

[150] Ibid.
[151] Ibid.
[152] Ibid.
[153] Ibid.

TikTok "Privacy Policy"[154]

While talking about the critical role that data privacy and security has in the core of the TikTok company, it is important to understand how these policies translate to the everyday use of the application. In addition to this, it is important to be certain that these policies are actually being understood by the users themselves, which is why emphasis is placed on the accessibility of this information for the everyday U.S. user, as well as the actual content. In terms of digital sovereignty, by giving the everyday American user more control over their data and giving users more access to this information, the more U.S. citizens' concerns will be quelled.

TikTok's "Privacy Policy" and information surrounding it come mainly from their website, which is broken up into three different categories: those who live in the United States, those who live in the U.K., E.U., and Switzerland, and those who live anywhere else. The United States' website is broken up into the following sections, "What information we collect," "How we use your information," "How we share your information," "Where we store your information," "Your rights and choices," "The security of your information," "How long we keep your information," "Information relating to children and teens," "Privacy Policy update," "Contact," and "Supplemental Terms – Jurisdiction-Specific."[155] The version used in this paper was last updated on August 4, 2023, which is interesting to note as it is after the TikTok hearing in the United States, which could have influenced their Privacy Policy or language used. Much of the document is in the format of paragraphs in bulleted form and written in plain language for people to understand. If users have more accessibility to a document like this, they are thus able

[154] "Privacy Policy," TikTok, *TikTok*, December 1, 2023. https://www.tiktok.com/legal/page/us/privacy-policy/en
[155] Ibid.

to understand what rights they have in terms of the application and can better apply them to their use of it.

Diving into the actual contents of the document, TikTok does collect a massive amount of data on users, but not quite as much as Instagram does in many ways.[156] While TikTok does collect data such as account information, generated content, messages, information in your devices' clipboard, contacts, purchase information, and choice preferences, much of this data has to be consented to before TikTok has access to it, rather than it being by default.[157] This plays into data privacy notions of being able to consent to data being collected.

In terms of what this data is used for, TikTok also does not use it for too many malicious purposes, just to customize ad experience, show suggestions, promote the platform, platform functionality, send promotional material, customize content, detect crimes, and "infer" things such as ages and preferences.[158] This furthers the idea of data collection minimization. According to this document, the data is not sold, but it is vague for how long this data is collected.[159] According to their privacy policy it is simply kept “as long as necessary,”[160] without the option to have anything deleted if you are over the age of 18.[161] In this sense, TikTok does not properly comply with a law like the CDPA, which explicitly protects the user right to deletion of any of their data, regardless of the circumstances.

One interesting thing to note about the pdf of the TikTok Privacy Policy, is that when downloaded there remains a link embedded into the pdf which brings you directly to TikTok’s

---

156 “Privacy Center.” *Meta.* December 1, 2023. https://privacycenter.instagram.com/policy
157 “Privacy Policy,” TikTok, *TikTok*, December 1, 2023. https://www.tiktok.com/legal/page/us/privacy-policy/en
158 Ibid
159 Ibid.
160 Ibid.
161 Ibid.

website. This logo obscures parts of the Privacy Policy and in order to try and identify or interact with the information covered by the logo, it is very difficult not to end up on TikTok's main website.

Most of the information on the way in which TikTok handles user data is in a more accessible format and found on a different website that is operated by TikTok, which will be examined in the following section. Because data security and data privacy are often critically linked, we are also exploring what TikTok has to say about their data security practices, which help from unwanted actors from accessing or manipulating data.

TikTok U.S. Data Security[162]

The first result that shows up for TikTok's Privacy Policy (a sponsored result) leads directly to a video by TikTok in English, with subtitles. It is important to note that this is *not* TikTok's Privacy Policy. It does, however, intend to inform its users and critics alike what TikTok's security measures are to protect U.S. user data. As observed in the following section, this page operates essentially as TikTok promotional content, and while it is important in explaining a lot of their data security policies, it doesn't necessarily give a lot of information.

The video starts of with "At TikTok we care deeply about the privacy and security of your data,"[163] setting the tone for a video that explains how TikTok is ensure the proper storage and usage of user data. It is here that the claim is made by TikTok that they are striving to have the "most secure"[164] social media platform on the Internet, similar to the statements made by Chew in March. TikTok goes on to explain the different ways in which they have created this

[162] "TikTok U.S. Data Security." *TikTok*. December 1, 2023. https://usds.tiktok.com/
[163] Ibid.
[164] Ibid.

"secure"[165] platform. The video lasts only 2 minutes and 13 seconds, which means that it is quite accessible to many users. This is important because in order to best protect one's data privacy, it is critical that there is proper understanding of the critical role that data security plays in this.

The website is called TikTok U.S. Data Security, and a plethora of information can be found here as it pertains to the way that TikTok handles user data. The page is split up into "News," "Media," "Research," "Myths vs Facts," "FAQ," and "About."[166]

The "News" section displays articles given by TikTok or other official members of the TikTok corporation (e.g. the Chief Operating Officer or the "Head of Trust and Safety") about updates regarding their data security protection.[167] All of these articles paint TikTok in a positive light, talking about topics ranging from TikTok's work on better securing user data to their development of research APIs in order to bring more transparency to the app.[168] It is important to note that all of these articles are written by TikTok, and none of them have comment or feedback sections. Other than the "contact" section on the bottom of the page, even in the "FAQ" section, there is no interactivity.

The "Media" section is full of recently published news articles, which all put TikTok in a good light as well. As of December 1, 2023, the first three articles are entitled "Don't Ban TikTok. Make It Safer for the Country," "Lawmakers Say That TikTok Is a National Security Threat, But Evidence Remains Unclear," and "ACLU Urges US Lawmakers Not To Ban TikTok, Citing Free Speech."[169] As of December 1, 2023, there were 39 articles on this section of the website. Articles varied in newsource (such as having the BBC and CNN), as well as in

---

[165] Ibid.
[166] Ibid.
[167] Ibid.
[168] Ibid.
[169] Ibid.

type (e.g. business and law reviews were also cited).[170] This is another way in which TikTok is using this sponsored website to selectively curate and promote its agenda. TikTok believes that it does not affect the digital sovereignty of the United States.

The "Research" section operates very similarly to the "Media" section, just having three research articles about the safety of TikTok usage, especially as it relates to a national security threat.[171] The "Myth vs Fact" section maps out 18 "myths" surrounding the way that TikTok governs its data, and responds to each of them with the "fact."[172] The "About" and FAQ" section continue on this note of promoting content that is favorable towards the views that TikTok is not only a secure social media platform, but also one that is pioneering in terms of data privacy for its users.[173]

Overall, this data security section of TikTok's massive internet presence is intended to make users feel more secure in giving their data to TikTok, resting assured that their data will only be used by the corporation itself, without the risk of malicious actors. This works towards TikTok's main goal of prevention of getting banned in the United States. While all of the words of Shou Chew, the privacy policy, and the data security website seem to paint TikTok in a positive light in which there is little room for foreign powers to access user data, the United States Congress feels differently.

The Congressional Committee on Energy and Commerce

The following section explores what the Congressional Committee on Energy and Commerce feels about the whole "issue" of TikTok. In doing a close textual and comparative

---

[170] Ibid.
[171] Ibid.
[172] Ibid.
[173] Ibid.

analysis of the memorandum from this committee, we can better understand how the two points of view are at odds with each other as it comes to the way that TikTok operates with data privacy and digital sovereignty.

The memorandum from the Congressional Committee on Energy and Commerce Democrats takes a much more serious and dire tone than Chew's testimony. In addition to the language itself being more professional, the format is better organized and sources are all included in footnotes (Chew's testimony had no sources).

The rhetoric in this memorandum is harsh, and there are superlatives throughout (e.g. TikTok collects more data "than any other social media app" or that Chinese employees have had "full access to and control over" U.S. user data).[174] There is a clear agenda here in trying to emphasize the dangers that TikTok poses to everyday U.S. citizens who use the application because of the issues they delineate.

The second section of the memorandum is entitled "TikTok and China," which focuses on China's relationship with TikTok and their parent company ByteDance. This sections explores the risks that are associated with ByteDance being based in the People's Republic of China, such as how the Chinese government has legal access to online data from Chinese companies. The U.S. congressional committee is proposing that TikTok is infringing on the digital sovereignty of the United States in this way. Evidence for this comes from a leaked employee meeting's audio, which stated that China has had historical access to this data.[175] Having access is one of the critical pillars of data privacy and digital sovereignty. If the Chinese

---

[174] Frank Pallone, "MEMORANDUM," *Energy & Commerce Committee Democrats*, March 21st, 2023, https://democrats-energycommerce.house.gov/sites/evo-subsites/democrats-energycommerce.house.gov/files/Minority_Memo_Full_Committee_Hearing_2023-03-23.pdf

[175] Ibid.

government truly has access to U.S. user data, this would be an infringement on U.S. data sovereignty. In addition to this, security concerns stem from the fact that the U.S. can be influenced by Chinese propaganda and public opinion.[176]

In a later section of this called "Data Privacy," which is under the section "TikTok Exemplifies Issues with Social Media," the congressional committee explores how the issue of data privacy and how social media companies infringe on it is not an issue unique to TikTok, however it emphasizes the dangers of TikTok specifically. As earlier stated, ultimately in many ways the issues of digital sovereignty stem from issues of data privacy at the individual level. The committee first acknowledges the precarious fact that the United States does not have a comprehensive national consumer privacy framework in place, and acknowledges how this leaves business "generally free to collect, use, share, and sell data without meaningful limits."[177] While in a sense very self-aware of the committee, it uses this fact to further explain why TikTok is dangerous specifically within U.S. borders. In order to make this issue sound even more extreme, the memorandum goes on to explain that information related to health, geolocation history, and even Social Security numbers are at stake.[178] They critically explain how consent is an important part of why this is bad, stating that data obtained by corporations like TikTok in the United States can be sold and used without direct user consent.[179] This first part of the "Data Privacy" section show that from the perspective of some sections of the U.S. Federal Government, TikTok is exploiting the lax nature of the laws.

---

[176] Ibid.
[177] Ibid.
[178] Ibid.
[179] Ibid.

In the second part of this section, the committee further expands on what a view of data privacy looks like in the United States. Citing the Federal Trade Commission's attempts to protect privacy against "unfair or deceptive acts or practices,"[180] the committee again emphasizes the current nature of the United States' laws or lack thereof. This shows that from at least the perspective of some Democrats, data privacy is not properly protected in the United States.

In evaluating what the Congressional Committee on Energy and Commerce has to say about the "issue" of TikTok, we can see how it emphasizes the risks of the lax laws in the United States and how these can be used in order to use data in malicious ways from foreign actors. On the other end, it is important to see what the People's Republic of China thinks about the accusations that they are unfairly using a private corporation to exploit American citizens.

Data Security in the People's Republic of China

As seen in the memorandum by the congressional committee and the statement made by Shou Chew, the main supposed abuser of U.S. data is the Chinese government. According to the congressional committee, the People's Republic of China has been able to exercise power over TikTok to obtain information from American citizens that would infringe on the digital sovereignty of the United States.

Starting in 2015, the People's Republic of China started to pass a series of interconnected laws that aimed at strengthening the national security, particularly as it related to the digital realm. In many ways however, their version of national security violates what many other countries, like the United States, view as their digital sovereignty. The National Security Law of the People's Republic of China was passed in July, and is made up of 7 sections containing 84

[180] Ibid.

articles.[181] The overall goals of the law included maintaining national security and defending the socialist system. It starts off with general provisions, then moves into tasks and duties in the preservation of national security. After this, it touches upon the National Security System, which is followed by national security safeguards, and then finishes with the duties and rights of citizens and organizations.[182]

Chapter I emphasizes the importance of maintaining national security in order to best defend the socialist system.[183] Nationalist sentiment is felt throughout the bill, but especially in this first section, with references to great revivals of China and the goals of the Chinese Communist Party.[184] Article 11 importantly states that "Citizens of the People's Republic of China, all state organs and armed forces, each political party and mass organization, enterprises, public institutions and other social organizations, all have the responsibility and obligation to preserve national security,"[185] which essentially encompasses all facets of the state into kowtowing to the Chinese Communist Party (Article 4 clearly states to adhere to the leadership of the CCP[186]). Enterprises are noted here to also have to oblige in preserving national security of the People's Republic of China[187], which is a reason for why many believe that corporations like ByteDance can be forced into compliance.

The rest of the law talks continues to emphasize the leadership of the Chinese Communist Party in maintaining the socialist system with Chinese characteristics.[188] The second chapter is

---

[181] "National Security Law of the People's Republic of China," *China Law Translate*, July 1st, 2015, http://www.chinadaily.com.cn/hqcj/zgjj/2015-07-01/content_13912103.html
[182] Ibid.
[183] Ibid.
[184] Ibid.
[185] Ibid.
[186] Ibid.
[187] Ibid.
[188] Ibid.

controversial because of some of the extreme measures it allows Beijing to take in the name of national security, such as through provisions of "strict"[189] punishments against terrorism. Other important provisions encourage giving the Chinese Communist Party leads on potentially harmful activities and limiting of rights during states of emergency or war.[190] Beijing makes it very clear in this law that there is no room for compromise outside of the direct views and guidance of the highest officials.

Following this in 2016, the Cybersecurity Law was passed, which offered a legal framework for ensuring Chinese cybersecurity, national sovereignty, and a healthy native technology industry.[191] As much as this functions as a law, it also functions as a call to action to encourage more citizens to participate in the cybersecurity of the country (e.g. educational institutions to participate in innovative programs to propel forward national standards).[192] The provisions in this act are wide in scope, varying from data localization to definitions of the security systems that need to be in place to ensure domestic cybersecurity.[193] Measures of the latter include obligations for internet service providers.[194] This is clearly an attempt by the People's Republic of China to establish their own form of digital sovereignty. Similar to the way that Project Texas proposes data localization, there are trends that indicate that data is no longer simply viewed as obscure and border free, rather it exists very expressly in a given territory that

---

[189] Ibid.
[190] Ibid.
[191] "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," *Stanford University*, June 29th, 2018, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/
[192] Ibid.
[193] Ibid.
[194] Ibid.

stores it. The Cybersecurity Law is thus another way in which a nation is attempting to bring their laws up to date into the middle of the 21st century.

In 2017, National Intelligence Law expanded on the overall cybersecurity framework in the People's Republic of China, and in many ways attempts to reach extraterritorially.[195] Out of the 32 articles that are outlined in this, the two most controversial outside of the People's Republic of China were articles 7 and 10. These two are critical in understanding the national security concerns of the United States as it relates to TikTok.

Article 7 states that all organizations and all citizens "shall support, assist, and cooperate with national intelligence efforts."[196] The concerns in this article is that the requirement for all members of the state to work towards the furthering of the national security agenda. With this, there seems to be a mass mobilization effort to protect the national intelligence effort, while the government also states that they will protect those who assist them.

This becomes more concerning when looked at alongside of the 10th article, which states that Chinese national intelligence institutions are to use any "necessary means, tactics, and channels to carry out intelligence efforts, domestically and abroad."[197] While the first part importantly shows that there is essentially no limit to what the Chinese government is willing to do to procure intelligence, the second part of this statement, specifically "and abroad" have much farther reaching implications. The People's Republic of China is willing to go through any means necessary to gain foreign intelligence information, and is legally able to require all citizens and organizations to do the same.

---

[195] Ibid.
[196] Ibid.
[197] Ibid.

In 2021, Data Security Law is another way in which the People's Republic of China is attempting to secure its digital sovereignty.[198] This law outlines the way in which data should be handled and secured, creating standardizations for any data-related activities.[199] The goal of this is to ensure data security, promote data protection, and to safeguard national security.[200] As stated, data security is a large part of digital sovereignty and data privacy. As the People's Republic of China attempts to standardize the securing of its native data, we can see how they are prioritizing data security in the digital world in the 2020s.

The final law that is important to note in 2024 for the purposes of better understanding Chinese digital sovereignty is the Personal Information Protection Law. Also adopted in 2021, this 74 article act explores the proper handling and processing of personal information.[201] Articles 38 and 39 have to do with the international processing of data, which is important to understand better the way in which the PRC views their digital sovereignty.[202] These two articles are important as they require that when personal information that is natively Chinese is processed outside of the borders of the mainland, there are extra provisions. For example, Article 39 explains that there needs to be reasons for the processing of the data overseas, as well as that the person who is requesting the information is identifiable and traceable.[203] As the Chinese government values the size of itself, this makes sense that in a Chinese version of digital

---

[198] "Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)," *Stanford University*, June 29th, 2021, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/
[199] Ibid.
[200] Ibid.
[201] "The PRC Personal Information Protection Law (Final): A Full Translation," *China Briefing*, August 24th, 2021, https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/
[202] Ibid.
[203] Ibid.

sovereignty there would be requiring more government oversight. In addition to this, it is interesting to note that in order to process data overseas, it is necessary that a person gives the Chinese government more of their personal information. In addition to this, Article 40 furthers the Cybersecurity Law's concept of data localization, mandating that processing for personal data of Chinese citizens stays within the territory of the People's Republic of China. Even if a foreign nation's courts mandate the data be processed, the Chinese government would need to approve of this, thus making themselves the sole controller of all data that is produced by their citizens. Essentially, the Personal Information Protection Law seeks to give the Chinese government more direct control over who is able to access data on their citizens.

While it is legally viable in the People's Republic of China to take information and data from foreigners by any means necessary, the People's Republic of China does not share their own data in the same way. The People's Republic of China does not hold itself to the same ethical standards as it forces onto other countries, as we will further explore as the Chinese Foreign Ministry responds to some of the TikTok controversies in the United States.

Reactions from the Chinese Foreign Ministry

The Chinese Foreign Ministry is part of the executive branch of the People's Republic of China, and responsible for the foreign relations of the Chinese state. The following section explores how the Chinese Foreign Ministry uses TikTok to whine about how the United States, acting as the global hegemon, treats Chinese companies unfairly.

The day directly after the TikTok hearing, Spokesperson Mao Ning held a regularly scheduled press conference. The question that was asked about TikTok came from Reuters, who

asked if there was "any comment"[204] about the hearing's conversations around Chinese influence over the platform and whether U.S. citizens' data is being shared. Ning responded:

> We have noted the remarks from TikTok. The Chinese government takes data privacy and security very seriously, which is under legal protection. The Chinese government has never asked and will never ask any company or individual to collect or provide data, information or intelligence located abroad against local laws. The US government has provided no evidence or proof that TikTok threatens US national security, yet it has repeatedly suppressed and attacked the company based on the presumption of guilt. We noted that some US lawmaker has said that to seek a TikTok ban is a "xenophobic witch hunt". The US should earnestly respect the principles of market economy and fair competition, stop suppressing foreign companies and provide an open, fair, just and non-discriminatory environment for foreign companies operating in the US.[205]

In this first addressing of the TikTok hearing, we can see a lot of different angles that the Chinese implement to try and deflect their own issues onto the United States. For one, they claim that the government has and never will ask to collect data from anyone. This is hard to believe because of Article 7 and 10 of National Intelligence Law, which explicitly states that that the Chinese government has the legal authority to do exactly this. It would be interesting to write this section out and then push to put this into a law if it was never intended to be used. The Chinese then accuse the U.S. government of having no proof that TikTok threatens national security, when in reality any data at all going to the Chinese government is a national security

---

[204] "Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on March 24, 2023," *Ministry of Foreign Affairs, the People's Republic of China,* March 24th, 2023, https://www.fmprc.gov.cn/eng/xwfw_665399/s2510_665401/2511_665403/202303/t20230324_11048722.html

[205] Ibid.

threat. The United States has a right to protect its citizens information from ending up in the hands of a government that is actively committing a genocide against its own citizens, among a host of other issues that the dictatorial regime has against human life and dignity.[206] [207] [208] Then, the Chinese reference a conversation with the TikTok CEO as "xenophobia," which is interesting to consider because the United States also does not have a history of being "xenophobic" to Japanese technology companies (e.g. Sony, Panasonic, Nintendo, etc.), Korean technology companies (e.g. Samsung), or really any countries who haven't explicitly stated that they would "take all measures necessary" to absorb a sovereign nation into its own territory, among other issues that the tyrannical never-to-be-a-global-hegemon has.[209] The last argument that the subject to the all-encompassing Chinese communist state about the United States not respecting the free market as the Chinese do is not worth getting into for the purposes of this thesis, as while there is no limit on length, there is a limit on years that I have in my life.

The 24th of March was a Friday, on the 27th, the following Monday, Mao Ning was asked to comment about legislation being brought forth involving TikTok. Ning responded again by attacking the United States. She states, "Keeping others down will not make oneself stronger,"[210] playing into the Chinese idea that they are in fact the underdogs who are being

---

[206] Waller, James, and Mariana Salazar Albornoz. "Crime and no punishment? China's abuses against the Uyghurs." *Geo. J. Int'l Aff.* 22 (2021): 100.
[207] Smith Finley, Joanne. "Why scholars and activists increasingly fear a Uyghur genocide in Xinjiang." *Journal of Genocide Research* 23, no. 3 (2021): 348-370.
[208] Bonardi, Mia. "More Problems from Hell: The Uyghur Genocide." *J. Glob. Rts. & Org.* 12 (2021): 1.
[209] Kyle Amonson, "The Ambitious Dragon: Beijing's Calculus for Invading Taiwan by 2030," *Journal of Indo-Pacific Affairs*, March 2023.
[210] "Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on March 27, 2023," *Ministry of Foreign Affairs, the People's Republic of China,* March 27th, 2023, https://www.fmprc.gov.cn/eng/xwfw_665399/s2510_665401/2511_665403/202303/t20230327_11049837.html

suppressed by the United States. She continues on to say that the United States should "stop suppressing foreign companies and provide an open, fair, just and non-discriminatory environment for foreign companies."[211]

The following day a Reuters reporter referred to a comment describing TikTok as a "Trojan horse,"[212] to which Mao Ning responded harshly.

> We've stated our position on this issue on multiple occasions. The US side has provided no evidence or proof to support its allegation, yet it has been abusing its state power to block and suppress the company concerned. This seriously violates the principles of market economy and fair competition, of which the US claims itself to be a champion. This is a classic example of US hegemonism. The US is hurting not just the interests of the company and the American people, but also its reputation as a nation and investor confidence in the US business environment.[213]

The frustration starts at the beginning, which is a similar fashion to which other TikTok-related questions got answered. Mao Ning uses harsh rhetoric, accusing the United States of "abusing" its state power. The Chinese Communist Party mouthpiece again states that there is no proof and that the United States does not respect its own rules. After calling the U.S. the hegemon, it is clear that this is Chinese insecurity as their position of the Great Power that will never be. We can clearly see in this response that the Chinese government is using the TikTok debate to accuse the United States' attempts at digital sovereignty as bullying, simply because the United States isn't afraid to call out the Chinese.

---

[211] Ibid.

[212]

[213] Ibid.

The final time that TikTok is mentioned in the days following the Congressional hearing is the question asked China Global Television Network, which is a Chinese state-run news channel. CGTN, a company under *direct* control of the Central Propaganda Department[214] asks Ning about the courtesy that foreign companies receive in China, versus how TikTok is faced in the United States. Essentially, in this question, the Chinese government asks itself a question that it wants to hear.[215] In one final opportunity to accuse the United States of foul-play, Ning states the following:

> You also mentioned the unfair treatment relevant companies have recently experienced in the US. I think many saw what happened. The US needs to earnestly respect the principles of market economy and fair competition, stop suppressing foreign companies, and provide an open, fair, just and non-discriminatory environment for the investment and operation of foreign companies in the US.[216]

Ning uses a harsh tone in this response, calling the U.S.'s treatment of foreign companies as "unfair," and stated that the United States is "suppressing" them. Ning continues to take the position that the United States is treating the rest of the world's corporations in a discriminatory way. It is interesting to see here, especially considering the fact that the U.S. federal government

---

[214] "Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on March 28, 2023," *Ministry of Foreign Affairs, the People's Republic of China,* March 28th, 2023, https://www.fmprc.gov.cn/eng/xwfw_665399/s2510_665401/2511_665403/202303/t20230328_11050458.html

[215] This is quite similar to how in the elementary school I would ask one of my friends to ask me an easy question to me to make me look good during my own presentations.

[216] "Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on March 28, 2023," *Ministry of Foreign Affairs, the People's Republic of China,* March 28th, 2023, https://www.fmprc.gov.cn/eng/xwfw_665399/s2510_665401/2511_665403/202303/t20230328_11050458.html

did not actually take any actions against TikTok as of this point. It is especially interesting to consider alongside the People Republic of China's long history of bullying foreign companies.

Overall, it is important to look into the People Republic of China's point of view in this because they are the reason for why the United States has felt the need to challenge TikTok. Without specific Chinese legislation in place, the United States would have no need to look into the app. While the People's Republic of China is good at blaming other countries for why they are disliked, they are unfortunately bad at being likable.

The Future of TikTok

While looking at the international TikTok debate, it is also critical to look at the ideas of digital sovereignty versus those of digital hegemony and the role that nationalism plays in this. It can be argued that the USA PATRIOT Act is just as far reaching in its scope as some of the acts passed in the People's Republic of China, especially as it relates to the international exploitation of data. While the United States is using this for purposes of anti-terrorism, however, the Chinese use their data to power algorithms to systematically eradicate minority groups.

Conclusion: The Best Ways to Protect Digital Sovereignty

Overview

Overall, this thesis intended to interact with the ideas of data privacy and digital sovereignty as they related to TikTok. I argued that the current U.S. policies which relate to the protection of user data is not sufficient for the expectations that many in the Western world hold for the control of their data. Because of this, many companies can legally collect and control massive amounts of data on their users without any legal repercussions. Personal individual user

data is being exploited by many different actors, however, and besides private social media companies, the U.S. government and international governments often have the legal right to obtain otherwise private data. While the U.S. federal government lags behind much of the developed world in terms of privacy protections, individual states have stepped up to fill in the gaps.

Virginia is a critical state in understanding what a privacy framework could look like in the United States, in compliance with U.S. laws and cultural customs. We can see how in the Virginia CDPA there are many different ways in which language that has already been used before in the United States continues to be used in the same way to best explain data privacy. Essential principles such as access, deletion, and minimization have been established on a national level in some specific pieces of legislation that are limited in scope. Virginia is also not unique in its approach to data privacy. Other states such as Connecticut and California have also established their own laws similar to the CDPA, showing that there is not only the capabilities for something like this to pass on a national level, but there is also the will. As it stands today, bad actors and foreign adversaries still can gain access to private information if proper data privacy and data security measures are not in place. Ultimately, much of U.S. data is up for grabs by the private sector, which easily can then be legally and forcefully taken into the hands of a variety of nation states in the name of national security. By learning from the way that Virginia operates now, including some of the cons that have been associated with implementation of digital sovereignty and data privacy laws, we can understand how to best apply a national framework to the country as a whole. It is important to consider the fact that major policies such as these will have consequences on some institutions such as educational institutions and private enterprises, however it is worth it to protect against the dangers of foreign adversaries.

The first chapter of this thesis explored the current landscape of U.S. data privacy policy. A look into these policies reveal that there are many gaps in explicitly protected data for U.S. citizens. Because of the lax laws in the United States at a federal level, it is easy for private corporations to exploit user data for their own profit. Negative implications of the private sector having massive amounts of data are that they can be legally obtained by the U.S. federal government and can easily be leaked when the proper data security measures are not put into place. While there is no comprehensive piece of data-protection legislation like there is in Europe or Japan, individual states have been able to work towards protecting their own constituents personal information.

This is critical to understand the current situation in the United States and why we have not yet passed a comprehensive data privacy legislation. Not only is it not directly in our constitution, but there are also ways in which the government itself benefits from the current data situation.

The second chapter looked at Virginia as a case study of what U.S. data privacy laws can look like in practice. While there are many different ways that a government can go about protecting the privacy and integrity of its citizens' data, there are also many impacts that laws can have on a variety of institutions. In the case of Virginia, pieces of legislation like the CDPA were beneficial in the comprehensive protection of Virginian user data, yet came at the cost of possibly inhibiting the growth of smaller businesses through extra regulations. In order to protect a semblance of digital sovereignty in the Commonwealth, executive orders and acts have been passed that attempt to take away the operational rights of companies based out of, or owned by other companies based out of, the People's Republic of China. While this is a smaller scale, there are still many different ways in which every day Virginians were affected. This second chapter

led into larger discussions of how a TikTok ban or any attempts to limit Chinese-owned companies from operating in the United States would functionally operate on a day-to-day basis.

This chapter is the most essential in understanding what the future could look like in the United States wherein the data privacy and digital sovereignty of the country is strongly protected. In both banning platforms that are owned by foreign adversaries and ensuring universal data privacy, the Commonwealth of Virginia is an example to the rest of the nation on what proper digital sovereignty could look like in a uniquely American way.

The final chapter of this thesis ultimately revolved around the ideas of digital sovereignty as it relates to the relationship between the United States and the People's Republic of China, using TikTok as a case study for how the general issue of digital sovereignty has expanded into the realm of the private sector. While both the United States and the People's Republic of China attempt to accuse TikTok of bending to the opposing government, TikTok believes that it should be able to operate fully and independently from far-reaching government regulation. CEO Shou Chew posits that data privacy is central to TikTok's mission, thus raising the question of whether or not a private corporation can truly be responsible for the protection of user data.

This final chapter is important because of the fact that we can use this to better understand the real dangers that come with such an open and free system in the United States. Because of the fact that there is not this comprehensive data privacy legislation, our digital sovereignty is at risk. The People's Republic of China realistically is either collecting our data, or has plans to because of the ways in which their laws have been structured. Because the People's Republic of China is a bad actor in the global arena for a variety of reasons, the United States needs to protect itself from such a threat.

Beyond the scope of this thesis, there are many considerations that have been left unanswered, which could be further explored. One interesting point that I did not get to include in this thesis was the idea that Taft brought up about the legality of something versus the ethics of it. While legally working within the scope of the law, social media platforms like Instagram and TikTok still collect a lot of data on its users. To what extent is it the role of private corporations to limit their data collection and usage, if at all?

In addition to this, there have been recently many calls to ban TikTok on a national level in some capacity in the United States. As already seen in states like Montana, TikTok bans can be tricky to logistically apply to the law. Luckily, the U.S. federalist system allows trial and error across various states, to see which are most effective and legally sound ways of preventing the ByteDance-owned application from causing more harm to Americans and their personal data than it already has.

Another interesting consideration is how this applies to countries besides the United States. Possible research into the state of digital sovereignty and data privacy as it relates to foreign adversaries could be explored with many different governments. The European Union and Japan, for example, have comprehensive privacy frameworks that aim to protect their citizens from mass exploitation like that which is found in the United States. Have these countries been inhibited in growth or otherwise because of stricter data privacy regulations and how do these regulations interact with private international organizations like TikTok who may be ceding legally collected information to foreign adversaries?

India, for example, is the largest country in the world to have banned TikTok. Further research can be done into what effects this has had on the nation, if any. Does it make them less

competitive on an international level because of some of the economic opportunities afforded by the fastest growing social media application?

This is important not necessarily because any given person's data is critically valuable to foreign adversaries, but because in aggregate, massive amounts of data can have far reaching implications. Especially sensitive data like financial and health data can speak to the wellbeing and strength of a nation as a whole. When data such as this is in the wrong hands, it could be used to effectively further the agendas of bad actors. Looking beyond just social media companies like TikTok, other technologies that are owned by the People's Republic of China can also be used to harvest data from Americans for the gain of our foreign adversary. For example, Chinese ownership of various infrastructures can give massive amounts of information about economic wellbeing of the country.

More research could be done on how the Chinese Communist Party and the government of the People's Republic of China treat foreign companies poorly, yet expect their companies to be treated kindly. In addition to this, it could be explored how the insecurity of the People's Republic of China as a perpetual second-rate middle power leads it to call the current global geopolitical situation "unfair." While it is difficult to do too much research into the Chinese Communist Party because of their secrecy and history of lying, perhaps one day there will be no more People's Republic of China who behaves this way.

Overall, however, this thesis intends to do a few things. It one, intends to inform the readers about the current dangers surrounding data privacy in the United States and what its implications are for the digital sovereignty of the nation as well. Overall, the second major intent of this thesis is to inform what data policy could look like on a federal level in the United States. By first showing in Chapter 1 that there is a gap in the legislation on a federal level, I then look

into specific Virginia laws as a case study of what the United States government *should* be doing. We can see that the language being used in the Virginia legislation is very similar to other pieces of legislation that we've seen in the United States in the past, yet they are limited in scope. Ultimately, this intends to better inform conversations of whether or not we can truly, as a nation, establish ourselves as digitally sovereign if we don't first have data privacy. The TikTok situation is just one place upon which we see our digital sovereignty being infringed, but shows a large gap in what we believe needs to be done, versus what is being done currently.

Bibliography

Abad, Germán Llorca, and Lorena Cano Orón. "How social networks and data brokers trade with private data." *Redes. com: revista de estudios para el desarrollo social de la comunicación* 14 (2016): 84-103.

Amonson, Kyle. "The Ambitious Dragon: Beijing's Calculus for Invading Taiwan by 2030." *Journal of Indo-Pacific Affairs*, March 2023.

Anderson, Katie Elson. "Getting Acquainted with Social Networks and Apps: It Is Time to Talk about TikTok." *Library Hi Tech News* 37, no. 4 (2020): 7–12.

Bazarova, Natalie N., and Zhao, Pengfei. "Individualistic Privacy Theories." in *The Routledge Handbook of Privacy and Social Media*. (Routledge, 2023). 16-24.

Scott Bomboy, "TikTok ban and the First Amendment," *National Constitution Center,* March 22nd, 2024, https://constitutioncenter.org/blog/a-national-tiktok-ban-and-the-first-amendment#:~:text=The%20judge%20was%20presented%20with,in%20the%20least%2Drestrictive%20manner.

Bonardi, Mia. "More Problems from Hell: The Uyghur Genocide." *J. Glob. Rts. & Org.* 12 (2021): 1.

Katharina Buchholz, “The Rapid Rise of TikTok,” *statista*, October 7th, 2022, https://www.statista.com/chart/28412/social-media-users-by-network-amo/

Boyd, Danah and Crawford, Kate. "Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon." *Information, communication & society* 15, no. 5 (2012): 662-679.

Brooks, Gina Marie Stevens, Stevens and HeinOnline U.S. Congressional Documents Library. *Data Brokers: Background and Industry Overview (RS22137)*. 22137 ed. S.l.: s.n.

Chang, Younghoon, Siew Fan Wong, Christian Fernando Libaque-Saenz, and Hwansoo Lee. "The role of privacy policy on consumers’ perceived privacy." *Government Information Quarterly* 35, no. 3 (2018): 445-459.

Cranor, Lorrie Faith, Candice Hoke, Pedro Giovanni Leon, and Alyssa Au. "Are they worth reading-an in-depth analysis of online trackers' privacy policies." *ISJLP* 11 (2015): 325.

Delaney, Kellie. "The USA PATRIOT Act and Privacy: A New Frontier of Mass Surveillance." *GP Solo*, vol. 37, no. 5, 1 Sep. 2020, pp. 34 - 37.

Douglas, William Orville, and Supreme Court Of The United States. U.S. Reports: Griswold v. Connecticut, 381 U.S. 479. 1964. Periodical. https://www.loc.gov/item/usrep381479/.

Fung, Brian. “Analysis: There is now some public evidence that China viewed TikTok data.” *CNN*. June 8th, 2023. https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html

Hirsch, Dennis D. "The glass house effect: Big Data, the new oil, and the power of analogy." *Me. L. Rev.* 66 (2013): 373.

Jaeger, Paul T., John Carlo Bertot, and Charles R. McClure. "The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act." *Government Information Quarterly* 20, no. 3 (2003): 295-314.

Kerr, Orin S. "The next generation communications privacy act." *University of Pennsylvania law review* (2014): 373-419.

Klug, Daniel, Morgan Evans, and Geoff Kaufman. "How TikTok served as a platform for young people to share and cope with lived COVID-19 experiences." *MedieKultur: Journal of media and communication research* 38, no. 73 (2022): 152-170.

Mayer-Schönberger, Viktor, and Cukier, Kenneth. *Big Data*. (Houghton Mifflin Harcourt, 2013). 6-7.

Mead, Margaret. “Neighborhoods and human needs.” *Children’s Environments Quarterly* 1, no. 4 (1984): 3-5.

Moreno, Sabrina, and Karri Peifer, “TikTok’s economic impact on Virginia,” April 8th, 2024, https://www.axios.com/local/richmond/2024/04/08/tiktok-s-economic-impact-on-virginia

Otto, Paul N., Annie I. Anton and David L. Baumer. "The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information." *IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Secur. Privacy*, vol. 5, no. 5, 1 Sep. 2007, pp. 15 - 14.

Petronio, Sandra. "Communication privacy management theory: What do we know about family privacy regulation?." *Journal of family theory & review* 2, no. 3 (2010): 175-196.

Regan, Priscilla M. "Old issues, new context: Privacy, information collection, and homeland security." Government Information Quarterly 21, no. 4 (2004): 481-497.

Roy, Jim. "Polis and Oikos in Classical Athens1." *Greece & Rome* 46, no. 1 (1999): 1-18.

Sagiroglu, Seref, and Duygu Sinanc. "Big data: A review." In *2013 international conference on collaboration technologies and systems (CTS)*, pp. 42-47. IEEE, 2013.

Smith Finley, Joanne. "Why scholars and activists increasingly fear a Uyghur genocide in Xinjiang." *Journal of Genocide Research* 23, no. 3 (2021): 348-370.

Stewart, Potter, and Supreme Court Of The United States. U.S. Reports: Katz v. United States, 389 U.S. 347. 1967. Periodical. https://www.loc.gov/item/usrep389347/.

Taft, William Howard, and Supreme Court Of The United States. U.S. Reports: Olmstead v. United States, 277 U.S. 438. 1927. Periodical. https://www.loc.gov/item/usrep277438/.

Tidy, Joe and Galer, Sophia Smith. "TikTok: The Story of a Social Media Giant." BBC. August 5th, 2020. https://www.bbc.com/news/technology-53640724.

Warren, Samuel and Brandeis, Louis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193-220.

Westin, Alan F.. *Privacy and Freedom*. Atheneum. 1967.

Zhang, Zongyi. "Infrastructuralization of Tik Tok: Transformation, power relationships, and platformization of video entertainment in China." *Media, Culture & Society* 43, no. 2 (2021): 219-236.

Zuboff, Shoshana. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30. no. 1 (2015): 75-89.

Act, Privacy. "Privacy Act of 1974." (2019).

Chapter 53. Consumer Data Protection Act, Code of Virginia, 2021, https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

CHILDREN'S ONLINE PRIVACY PROTECTION, U.S. Code 15 (2011), §§ 6501-6506. https://www.govinfo.gov/app/details/USCODE-2011-title15/USCODE-2011-title15-chap91.

Electronic Communications Privacy Act of 1986. Public Law 508. U.S. Statutes at Large 100 (1986): 1848-1873. https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1848.

Electronic Communications Privacy Act. Code of Virginia. 2016. https://lis.virginia.gov/cgi-bin/legp604.exe?171+sum+SB599

Fair Information Practice Principles (FIPPs), U.S. Federal Government, 2022, https://www.fpc.gov/resources/fipps/

"Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on March 24, 2023." *Ministry of Foreign Affairs, the People's Republic of China.* March 24th, 2023. https://www.fmprc.gov.cn/eng/xwfw_665399/s2510_665401/2511_665403/202303/t20230324_11048722.html.

"Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on March 27, 2023." *Ministry of Foreign Affairs, the People's Republic of China.* March 27th, 2023. https://www.fmprc.gov.cn/eng/xwfw_665399/s2510_665401/2511_665403/202303/t20230327_11049837.html.

"Foreign Ministry Spokesperson Mao Ning's Regular Press Conference on March 28, 2023," *Ministry of Foreign Affairs, the People's Republic of China,* March 28th, 2023, https://www.fmprc.gov.cn/eng/xwfw_665399/s2510_665401/2511_665403/202303/t20230328_11050458.html

"In re: Choicepoint, EPIC, https://epic.org/documents/choicepoint-2/

"National Security Law of the People's Republic of China." *China Law Translate*. July 1st, 2015. http://www.chinadaily.com.cn/hqcj/zgjj/2015-07-01/content_13912103.html.

Office of the Federal Register, National Archives and Records Administration. "Public Law 104 - 191 - Health Insurance Portability and Accountability Act of 1996". Government. U.S. Government Printing Office, August 20, 1996. https://www.govinfo.gov/app/details/PLAW-104publ191

Office of the Governor of the Commonwealth of Virginia, *BANNING THE USE OF CERTAIN APPLICATIONS AND WEBSITES ON STATE GOVERNMENT TECHNOLOGY* by Glenn Youngkin. (Richmond, Virginia, 2022).

Personal Information Privacy Act, Code of Virginia, 2011, https://law.lis.virginia.gov/vacodepopularnames/personal-information-privacy-act/

"The PRC Personal Information Protection Law (Final): A Full Translation," *China Briefing*, August 24th, 2021, https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms. House of Representatives Energy and Commerce Committee, 2023. https://www.c-span.org/video/?526609-1/tiktok-ceo-testifies-house-energy-commerce-committee-hearing.

TikTok Team. "Celebrating our thriving community of 150 million Americans." TikTok, March 21st, 2023. https://newsroom.tiktok.com/en-us/150-m-us-users

"Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)." *Stanford University*. June 29th, 2018. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

"Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)." *Stanford University*. June 29th, 2021. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/

U.S. Congress. House. Protecting Americans from Foreign Adversary Controlled Applications Act. H.R. 7521. 118th Cong., 2nd sess., Engrossed in House March 13, 2024. https://www.govinfo.gov/app/details/BILLS-118hr7521eh.

U.S. Congress. House. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. HR 3162. 107th Cong., 1st sess. Introduced in House October 23, 2001. https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162ih/pdf/BILLS-107hr3162ih.pdf

United States. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 or FISA Amendments Act of 2008. [Bethesda, MD :ProQuest], 2011.

Virginia Congress, *Chapter 768*, 2023 session, https://lis.virginia.gov/cgi-bin/legp604.exe?231+ful+CHAP0768

Waller, James, and Mariana Salazar Albornoz. "Crime and no punishment? China's abuses against the Uyghurs." *Geo. J. Int'l Aff.* 22 (2021): 100.

Weiss and HeinOnline U.S. Congressional Documents Library. *Yahoo Data Breach - Issues for Congress (IN10586)*. 10586 ed. S.l.: s.n.