The Weaponization of TikTok

Understanding China's Sharp Power and Western Defense

Author
Ruth Beatrice Green

MA in Public Policy: Global Public Policy
Erasmus Mundus MAPP 2019-2021

In partial fulfillment of the requirements for the degree of ERASMUS MUNDUS MASTER IN PUBLIC POLICY

CEU Supervisor: Thilo Bodenstein
IBEI Supervisor: Pablo Pareja Alcaraz

Barcelona, Spain

July 2021

Authors Declaration

I hereby certify that this dissertation contains no material which has been accepted for the award of any other degree or diploma in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text.

I hereby authorize IBEI and Mundus Mapp Consortium the non-exclusive license to archive and provide my dissertation in whole, or in part, in all forms of media now or hereafter known. I retain the right to use in future works all or part of this dissertation.

Name: Ruth Beatrice Green

Signature: _Ruth B. Green____

Location and Date: Barcelona, July 10th, 2021.

Word Count: 13,067

Abstract

This MA thesis analyzes the characteristics of sharp power, a new tool of influence from autocracies to democracies, through the modern Chinese-owned social media app TikTok. It will look at the operationalization of TikTok through a case study approach with the United States of America (US) and the European Union (EU). Data governance is the strongest defense to sharp power by protecting domestic users from foreign intervention. The US and EU have two differing approaches to data governance with the US offering sector-specific laws and the EU's extensive data privacy regime. The two cases are analyzed through their extensive background with China's technology, similar user profiles, and increased concern over TikTok weaponizing user data to manipulate society. The case study adds to the sharp power framework by analyzing established governance institution within the modern tool. It concludes that the European Union has an extensive data privacy accountability structure that provides user protection, but is vulnerable to hidden, integrated influence as TikTok collects data via new invasive methods. The US has very little data protection and users are signifigantly more at risk than within the EU, as it fails to define data privacy norms or create an accountability structure for user concerns. The research offers policy recommendations centered around the need for a global data governance structure to protect users from a hidden coercive influence of harmful actors hidden through TikTok's business model.

Acknowledgements

I would like to thank my advisors, Thilo Bodenstein and Pablo Pareja Alcaraz for their advice to propel my thesis forward. I would also like to thank my family and friends for their encouragement and support during the writing process

Table of Contents

List of Abbreviations

AI	Artificial Intelligence
ASPI	Australian Strategic Policy Institute
BEUC	Bureau Européen des Unions de Consommateurs
CCP	Chinese Communist Party
CCPA	California Consumer Privacy Act of 2018
CFIUS	Committee on Foreign Investment in the United States
COPPA	Children's Online Privacy Protection Act of 1998
DPC	Data Protection Commission
EU	European Union
FERPA	Family Educational Rights and Privacy Act
FIRRMA	Foreign Investment Risk Review Modernization Act
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
ICIJ	International Consortium of Investigative Journalists
OECD	Organization for Economic Co-operation and Development
PII	Personally Identifiable Information
US	Unites States of America

Chapter 1: Introduction

1.1 Introduction

Social media is facing a dilemma as it has evolved from an easy way to pass the time to becoming a security issue for thousands of global users. The new social media app TikTok, by the Chinese company ByteDance, has created a foreign frenzy as the exported app exploded across western markets. Technology experts have begun criticizing the apps exploitation of user data, citing issues of national security and data privacy, classifying it as a new modern weapon of asymmetrical power relations. Recent studies have analyzed its capacity to infiltrate foreign markets and promote coercive agendas by the Chinese government across a widespread audience. This is a security issue for three key reasons: the unchallenged capacity for influence via social media in western markets, the rise of TikTok among younger users, and the lack of a global data governance regime to protect users across borders.

Data becomes a tool for influence as businesses with a large user base can utilize data collection and artificial intelligence (AI) processing to understand user preferences and provide more individualized content. From a security standpoint, this allows foreign data collectors to aggregate data about a specific population without any global infrastructure regulating how cross-border data can be used and processed. A 2018 report by the US National Endowment for Democracy defined this as data weaponization, creating the term Sharp Power to define this new method by autocratic regimes that "pierces, penetrates, or perforates the political and informational environments in the targeted countries".[1] Sharp power is autocratic regimes weaponizing large sums of data collected by businesses like TikTok to shift norms, manipulate perceptions, and promote rifts within society.[2]

There is a literature gap connecting the capacity of TikTok as a sharp power mechanism and the national-led data governance structures that protect users from harmful social media influence. To meet this gap, this thesis will first validate TikTok as a weapon of sharp power by outlining the role of autocratic regime agendas in the app infrastructure enabling it to influence users. Secondly, the thesis will compare two established data governance infrastructures, the United States (US), and the European Union (EU), to analyze

[1] Michael J. Cole, "THE HARD EDGE OF SHARP POWER: Understanding China's Influence Operations Abroad," (October 2018): 4, https://macdonaldlaurier.ca/files/pdf/20181022_MLI_China's_Influence_(Cole)_PAPER_WebreadyF.pdf.

[2] Christopher Walker, and Jessica Ludwig, "Sharp Power Rising Authoritarian Influence." *Journal Endowment for Democracy*, no. International Forum for Democratic Studies (December 2017): 11.

how differing national governance regimes can protect users. TikTok is highly mainstreamed in these cases as there are currently over 100 million TikTok users in Europe and 65.9 million in the US.[3] These two cases have different approaches to data norms, making them a relevant most-similar case study approach to understand how they can protect users from sharp power pressures. The focus will compare the role of the data governance regimes to create global data rights norms and their regulatory protection through business regulation.

1.2 Research Question

A main research question emerges. The field of sharp power is relatively new, making it important to analyze the social media app TikTok within the theoretical parameters of sharp power. The theoretical foundation of sharp power is also somewhat vague making it relevant to specify the social media app TikTok as a vector of influence in ways that other data-collecting social media apps are not. The main research question is as follows:
"What are the implications of the popular social media app TikTok being used as a vector of foreign influence on individual users in democratic societies?"

To properly analyze the long-term implications, a case study emerges, to compare two major norm-setting data governance bodies, the US and the EU within the example of TikTok as a mechanism of influence. The sub question then becomes:
"How do the current democratic institutions protecting data privacy laws protect users from the influence of sharp power through the Chinese social media app TikTok?"

1.3 Research Aim

The aim of this research is to define modern power relationships and digital governance networks through the framework of sharp power. Democratic governments have relevant data privacy governance structures and normative influence, but are they enough? To answer this question, the thesis will first validate the theoretical framework of sharp power within the case of TikTok, and then compare the normative data governance structures of two influential western democracies against the threat of TikTok. The case study compares the US and EU data protection regulations to analyze how they protect the average user, and how they define national level data governance in the fight against data weaponization.

This research adds to existing sharp power research, and data governance research, by analyzing a modern tool through existing frameworks. While TikTok is still a new method of

[3] Mansoor Iqbal, "TikTok Revenue and Usage Statistics (2021)." *Business of Apps*, July 2, 2021. https://www.businessofapps.com/data/tik-tok-statistics/.

data processing, it has created a new type of social media that is likely to be continued in the future years as other apps adopt similar algorithm processes. It is necessary to understand the holes in the current data governance infrastructure to develop policy recommendations to meet continued technology advances and apps of similar aptitude as TikTok.

The thesis has six sections. Section one provides an overview of the scope of the problem, the research gaps this thesis aims to fill, and an introduction into the thesis. Section two includes a literature review developing the foundation of sharp power and an overview of data sovereignty literature. Section three discusses the thesis methodology, including the research question, theoretical framework, the case study approach of the US and EU, and how this research adds to the academic literature on data governance. Section four discusses the case of TikTok by providing justification for TikTok as a weapon of influence through user data. Section five analyzes the case studies, looking at both the EU data privacy regime and the US data privacy regime to discuss gaps in the governance structures. Section six finishes the analysis with key findings, concluding that the EU is much more adept at protecting users and the US requires a massive overhaul of data privacy regulations to meet modern security risks. Next, it provides policy recommendations for the EU, US, and for general data governance.

Chapter 2: Literature Review

2.1 Defining Power Relationships: Hard, Soft, and Sharp Power

When defining power in terms of analysis, as this thesis aims to do, it becomes important to separate the normative assumptions of what constitutes power from the actors involved as context shifts the relevance of analysis.[4] A researcher, Dowding (2012), defines power as the study of actors, governmental or non-governmental and their influence on others, most understood as a zero-sum game.[5] Joseph Nye (2008) simplifies that "power is the ability to influence the behavior of others to get the outcomes one wants".[6] When evaluating the intentional use of power by nations, a divide arises as tactics deemed coercive in democracies are considered soft influence in authoritarian regimes. This divide in how methods are used, and the attempted influence makes the discussion of power relationships including the US, EU, and China require additional explanation for the terms used. Additionally, the discussion of traditional power, namely hard and soft power, are highly concentrated in western academic research and have a gap when utilized in power relationships of authoritarian to democratic societies. A review of traditional hard and soft power in authoritarian contexts is necessary to understand the emergence and legitimacy of sharp power as a modern tool.

Hard power is utilized within power relationships through tools of divisive influence and coercion, creating a positive asymmetrical power balance for one actor enacted on a secondary actor. It is an empirical tool for analysis, commonly through military and economic recourses, threats, and legal action.[7] It has important threads through many traditional theories of power, namely realism, but also liberalism and constructivist schools of thought. Researchers Beeson and Xu (2016) refer to the democratic use of hard power as regional economic ties, hegemony across economic institutions, the distribution of hard military power, and the capacity to exercise such power.[8] An academic article by Li, Zhang, and Hart (2018) defined China's hard mechanisms through their targeted economic trade and security, relying on strong bilateral and multi-national trade agreements as methods of coercive influence rather than liberal economic governance structures like the International

[4] Keith Dowding, "Why Should We Care about the Definition of Power?" *Journal of Political Power* 5, no. 1 (2012): 122. https://doi.org/10.1080/2158379x.2012.661917..

[5] Ibid., 120.

[6] Joseph S Nye, "Public Diplomacy and Soft Power." *The Annals of the American Academy of Political and Social Science* 616 (2008): 94. Accessed July 8, 2021. http://www.jstor.org/stable/25097996.

[7] Dowding, "Why Should We Care about the Definition of Power?," 130.

[8] Mark Beeson and Shaomin Xu, "Leadership with Chinese Characteristics: What Role for Soft Power?" *Global and Regional Leadership of BRICS Countries*, (2016): 174. https://doi.org/10.1007/978-3-319-22972-0_10.

Monetary Fund, or World Trade Organization.[9] China has demonstrated different goals with power relationships, utilizing economic channels and trade competition as the main source of hard power. [10] The military power is mainly used as a regional coercive tool, with researchers noting China's hard power agendas may use economic or military power, but refrain from both when applying tools of coercion.[11]

Joseph Nye coined the term 'soft power', a tool of influence including all tools that exist outside of military and economic force, namely culture, political values, national cohesion, and institutional legitimacy.[12] One of the most important tenants of soft power is the capacity for actors to provide influence and information via channels of trust.[13] However, the concept of soft power is commonly analyzed across a highly westernized normative conception of power making it difficult to apply to authoritarian regimes such as China, as the values and cultural norms are so different, disrupting the explanatory power of soft power itself.[14] While Nye assumed the US was the natural leader of soft power when he developed the term, more recent academic discussion began to shift this discourse by analyzing the slow decline of US soft power in the post-9/11 foreign policy.[15] When applying these terms of soft power to authoritarian regimes such as China, gaps emerge, as influence exerted is often considered more manipulative, and less reliant on trust, and generally more covert. Researchers at the University of Wollongong (2019) found that this gap can be accounted to the normative assumptions of soft law, and how they fail to properly define the mechanisms more present in authoritarian regimes such as China. Chinese leaders view the concept of soft power through their influence in spreading their ideology, and importantly, influencing other actors to see the 'correct' view of society in line with China.[16] Researcher Weihong Zhang (2010) concludes that China prioritizes recourses that are already disseminated, like TV channels such as *People's Daily*, and *Global Times*, and ensures they only discuss the culture

[9] Minghao Li, Wendong Zhang, and Chad Hart. "What Have We Learned from China's Past Trade Retaliation Strategies?" *Choices* 33, no. 2 (2018): 4. Accessed July 27, 2020. www.jstor.org/stable/26487436.

[10] Maral Noori, Daniel Jasper, and Jason Tower. Report, US Institute of Peace, 2015. Accessed July 8, 2021. http://www.jstor.org/stable/resrep20190: 2.

[11] Robert Sutter, "Barack Obama, Xi Jinping and Donald Trump—Pragmatism Fails as U.S.-China Differences Rise in Prominence." *American Journal of Chinese Studies* 24, no. 2 (2017): 76. Accessed July 14, 2021. http://www.jstor.org/stable/44759210.

[12] Beeson and Xu, "Leadership with Chinese Characteristics: What Role for Soft Power?," 175.

[13] Nye, "Public Diplomacy and Soft Power," 95.

[14] Dowding, "Why Should We Care about the Definition of Power?," 121.

[15] Beeson and Xu, "Leadership with Chinese Characteristics: What Role for Soft Power," 8.

[16] Brian Yecies, Michael Keane, Haiqing Yu, Elaine Jing Zhao, Peter Yong Zhong, Susan Leong, and Huan Wu, "The Cultural Power Metric: Toward a Reputational Analysis of China's Soft Power in the Asia-Pacific." *Global Media and China* 4, no. 2 (May 30, 2019): 206. https://doi.org/10.1177/2059436419849724.

and national values while avoiding topics of contention.[17] This exemplifies the inherent difference between western understanding of soft power, and an authoritarian regime's, as the line between influence and coercive knowledge is blurred.

2.2 Modern Power Relationship Theory: Sharp Power

Sharp power is a new approach to power relationships in the field of authoritarian power studies. Most reports are by institutions studying democratic securitization, with a lens colored by geopolitical interests. The first influential report on the concept of sharp power was through the US National Endowment for Democracy (2017), which describe it as a targeted tactic used by autocratic actors to directly influence foreign actors via "political and informational environments".[18] Sharp power influence by authoritarian regimes mainly acts through targeted destabilization methods on democracies to shake the trust and information channels that democratic societies value. This includes news outlets, social media disinformation campaigns, and weaponizing aggregated data to maximize influence.[19] Sharp power analysis generally follows five key tenets created by the Sharp Power Rising Authoritarian Influence Report (2017), that include manipulation, censorship, propaganda, control, and influence.[20] Most sharp power discussions revolve around Chinese and Russian infiltrated influence. A more recent discussion of sharp power, by Thomas Biersteker (2020), introduces a school of thought that looks at the potential of sharp power through influence the EU exerts. This analyzes the coercive and manipulative nature of western actors using sanctions and strengthening the Euro as a tool of influence. The literature for sharp power is almost solely based in western normative power theory, thus leading to most sharp power analysis to be used in a descriptive discussion of authoritarian actions on democratic societies, and limited research into alternative formats.

2.3 Data Sovereignty within Global Data Governance

Data affects all levels of actors, from individual to corporate and government actors. Researcher Liu (2021) defines data through its valuation problems across national and multinational actors, creating issues of credible commitment and partial excludability on an

[17] Yecies, Keane, Yu, Jing Zhao, Yong Zhong, Leong, and Wu, "The Cultural Power Metric: Toward a Reputational Analysis of China's Soft Power in the Asia-Pacific," 206.
[18] Cole, "THE HARD EDGE OF SHARP POWER: Understanding China's Influence Operations Abroad," 10.
[19] Thomas Biersteker, "The Potential of Europe's Sharp and Soft Power." *Global Policy* 11, no. 3 (May 18, 2020): 384–87. https://doi.org/10.1111/1758-5899.12815.
[20] Walker and Ludwig, "Sharp Power Rising Authoritarian Influence," 18.

international scale.[21] In recent years national governments have recognized the danger of data, but also the conflicts that arise when trying to securitize it within domestic channels. Data represents a commitment problem that requires individual-level governance. Once users exchange their data for goods and services online, usually offered in a free format for the cost of data, collectors can reuse it indefinitely as a nonrival good. It provides multinational firms with the power to disseminate their data, through channels of selling, trading, or processing. Thus, Liu notes the three challenges that make it impossible for a widely accepted data definition, as it is a problem of externality, commitment, and valuation.[22]

Data sovereignty thus becomes difficult for national governments and corporate actors to regulate allowing private companies complete power of exclusion to agree or disagree with data requests by other actors and government entities. A researcher Floridi (2020) defines sovereignty as "a form of legitimate, controlling power".[23] Floridi argues that the traditional definition of sovereignty fails in application to data, as the data individuals create is easily transferred cross-border, self-regulated, and without global checks and balances or market-based equilibria.[24] Floridi concludes that due to this, it becomes impossible for national governments to protect individual data sovereignty at a national or global level, but instead it must be given to the individual as self-ownership.[25]

Data governance struggles to define data sovereignty across borders as it is highly quantified by norms-based preferences at the domestic level. Data governance is considered a national securitization issue and is controlled by domestic politics that steer multinational companies' power of data through its access to domestic markets and costs of compliance.[26] Data privacy regulations and accountability structures are the first barrier of defense against a company's access to weaponizing data, by limiting covert collection methods and data processing. Governments with weaker or inaccessible data governance structures are more open to security issues without legal privacy transparency laws.

[21] Lizhi Liu, "The Rise of Data Politics: Digital China and the World." *Studies in Comparative International Development*56, no. 1 (March 19, 2021): 56. https://doi.org/10.1007/s12116-021-09319-8.
[22] Ibid., 47.
[23] Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *SSRN Electronic Journal*, August 12, 2020, 372. https://doi.org/https://doi.org/10.1007/s13347-020-00423-6.
[24] Ibid.
[25] Ibid.,371
[26] Ibid.

Chapter 3: Methodology

The methodology will rely on data collection through secondary sources, which include government documents, academic publications, journal articles, newspaper articles, laws, and organizational reports. As TikTok is a social media app, the use of recent reports and newspaper reports provides relevant perspectives and validations that aid in the discussion of TikTok as a sharp power tool. It is important to note that the discussion of TikTok as a sharp power tool is almost exclusively analyzed through academic and organizational reports, as well as newspaper articles. Sharp power is not widely established or acknowledged in power relationship studies, as it is relatively new with a narrow scope of analysis.

The theoretical framework will utilize sharp power as an explanatory mechanism. The combination of newspaper reports, personal accounts and academic discussions have created a framework for studying sharp power through five main tenets. The discussion will rely on common perceptions of western academic analysis and the western lens of analyzing power relationships. This introduces potential bias as the concept of sharp power is not recognized in autocratic academic fields but is only discussed in western academia. The thesis will first establish the theoretical foundation for sharp power within the realm of TikTok using the five tenets (e.g., manipulation, censorship, propaganda, control, and influence), and then analyze how TikTok interacts within the data privacy regimes of the US and EU. The aim is to understand the capacity of defensive institutions in the modern social media age, and implications for the future of power relationships.

The conceptual framework is more nuanced, relying on a case study of the US and EU data protection regimes as defense mechanisms against TikTok as a sharp power. The two chosen cases for the case study analysis are the United States and the European Union between the years 2015 to 2021. The US and EU have regulatory mechanisms in place that provide stable environments for technology platforms such as TikTok, as well as wide user bases that are adept at new apps and trends.[27] The case study selection aims to minimize selection bias by choosing cases that have similar technology backgrounds, and historical power relationships with China, allowing for a stronger analysis into the data regulatory schemes themselves with minimized historical background validation necessary. Both have established themselves as global norm-setting institutions in the technological competition

[27] Augusto Valeriani, and Cristian Vaccari, "Accidental Exposure to Politics on Social Media as Online Participation Equalizer in Germany, Italy, and the United Kingdom." *New Media & Society* 18, no. 9 (2016): 1861. https://doi.org/10.1177/1461444815616223.

sphere by setting standards across innovation and user reliance, creating a skewed balance of power as these two cases historically dominate the field.[28] Additionally, US and EU experts have discussed growing fears about the increasing digital illiteracy making users vulnerable, and the decline of core aspects of democracy across digital representation, such as independent, trustworthy journalism, weakened public institutions, and the impact of technology giants in data privacy policy making.[29]

A case study is defined by George and Bennet (2005) as "the detailed examination of an aspect of historical episode to develop or test historical explanations that can be generalized to other events".[30] This emphasis across case study research relies on "structured, focused comparison" through theoretical questions, attempting to connect an analytical question to a specific event or relationship.[31] The goal of this thesis is to analyze the current security risk of TikTok within established infrastructures, in a theory-led inquisition on how data governance structures can be generalizable as types of defense mechanisms. A case study was chosen for this analysis due to the modern, and relatively new theoretical framework that constitutes sharp power, as it is still a narrow scope of power relationships that is difficult to explain under wider conditions. The case study aims to redefine sharp power and offer a new strategy of analysis to better understand how it can infiltrate foreign actors. This thesis relies on a most similar case study method, defined as two similar cases with relevant background conditions except for X, and the outcome Y. What will be specifically analyzed is the differences in X, and how they can impact the outcome of Y.[32] The X variable will discuss the data regulation schemes present in the US and EU, comparing their regulatory and accountability bodies, as well as user satisfaction. The aim is a holistic view of the regulatory schemes within global technology security risks. The outcome, Y, will conclude the overall protection the data regulation schemes have for the average TikTok consumer, to analyze the roles national governments have in protecting users from the new concept of sharp power.

[28] Ingrid Schneider, "Democratic Governance of Digital Platforms and Artificial Intelligence?" *JeDEM - eJournal of eDemocracy and Open Government* 12, no. 1 (July 2020): 11. https://doi.org/10.29379/jedem.v12i1.604.

[29] Ibid., 5.

[30] Jack S. Levy, "Case Studies: Types, Designs, and Logics of Inference." *Conflict Management and Peace Science* 25, no. 1 (March 1, 2008): 2. https://doi.org/10.1080/07388940701860318.

[31] Ibid.

[32] Jason Seawright, and John Gerring, "Case Selection Techniques in Case Study Research." *Political Research Quarterly*61, no. 2 (June 2008): 304. https://doi.org/10.1177/1065912907313077.

Chapter 4: China, Sharp Power, and TikTok

4.1 A Sharp Power Analysis: The Case of TikTok

Sharp power is an explanatory concept almost exclusively used in relation to authoritarian actors optimizing information channels within democratic states as an opening for manipulation and influence. The goal is to shift narratives and knowledge across systems of trust to sow suspicion and decrease the legitimacy of targeted institutions and actors. This is especially powerful when weaponized against democratic societies as they value norms such as openness, free speech, and access to information within public institutions, media, and newspapers.[33] As today's access to information is so decentralized, from social media to online news outlets and even advertisements, it is difficult for democratic societies to realize the targeted weaponization of certain perceptions until they are already in effect.[34]

What marks sharp power different from soft power is that it utilizes authoritarian tactics to subtly control society and public opinion, such as top-down censorship, disseminating consistent pro-government rhetoric, and the mix between economic market values and government initiatives. It infiltrates public opinion across democratic society at an individual level, changing the common perceptions in a slow, unknowingly coercive tactic.[35] Sharp power exploits democratic values, using open-access information streams and a highly decentralized information society. It allows as authoritarian countries to use values of free speech to manipulate foreign societies, while also permitting authoritarian regimes to protect their own society through closed domestic data borders. Thus, it creates an asymmetrical information flow that experts consider especially harmful.[36] Sharp power has predominantly been documented across established democracies such as the US and EU, as well as within developing democracies across Latin America and Africa.[37]

Sharp power has a growing following across western academics; however, China and Russia argue that sharp power is a term created to villainize information campaigns promoted by autocratic countries. Chinese experts refer to sharp power as hypocritical, as democratic governments like the US and EU have launched their own extensive pro-democracy information campaigns for decades.[38] China has been a documented user of information

[33] Walker and Ludwig, "Sharp Power Rising Authoritarian Influence," 11.
[34] Ibid.
[35] Ibid., 13.
[36] Ibid., 11.
[37] Ibid., 20-21.
[38] Jingkai Shao, "Exploring China's' Sharp Power': Conceptual Deficiencies and Alternati." *Transcommunication* 6, no. 2 (September 15, 2019): 135. https://doi.org/https://www.researchgate.net/publication/335960974_Exploring_China%27s_Sharp_Power_Conceptual_Deficiencies_and_Alternatives.

campaigns for decades. It is necessary to understand the mix of government and business interests in the core foundation of China's agendas, mixing the Chinese Communist Party (CCP) with all economic sectors.

4.2 The Mix of China's Infrastructure and Sharp Power Campaigns

China has very different perceptions on norms and regulations for data collection, individual protection, and subtle data processing to promote government initiatives. This creates one of the major concerns western democracies have over imported Chinese technology, as there is no legal barrier between private collection of data, and government utilization. Western researchers have defined a norm across China that the use of data collection to identify and classify segments of the society is considered a public right, and a function of the party ideology. This assumes a right for the CCP to analyze and weaponize data from domestic social media apps against Chinese society to promote the progress and ideas that are conducive to government control.[39] Chinese owned technologies collect data through exported apps by offering services with user-engagement, like social media and media outlets. Data can then be weaponized by government actors to "read public sentiment and use language more effectively" across information campaigns.[40] In 2019, the BBC discovered extensive edits across Mandarin-language articles that shifted the article narratives to support the agendas the CCP prefers, such as changing the language associated with Tiananmen square to support CCP rhetoric, and editing Taiwan's Wikipedia page from describing it as "a state in East Asia" to "a Province in the People's Republic of China".[41] Another example includes a 2019 report by The International Consortium of Investigative Journalists (ICIJ) which discussed security risks they discovered across the CCP's use of data recourses, showing the CCP wielded extensive domestic social control through mechanisms of data collection and AI processing. The CCP could accurately collect individual consumer data on a mass level and use it to identify 'opposition to the state'.[42] What can be noticed through these mechanisms is the power of the CCP to censor and manipulate to create

[39] Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion." *Australian Strategic Policy Institute* 21 (October 2019): 18. https://doi.org/https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

[40] Ibid., 6.

[41] Christopher Walker, Shanthi Kalathil, and Jessica Ludwig, "The Cutting Edge of Sharp Power." *Journal of Democracy*31, no. 1 (January 2020): 124. https://doi.org/10.1353/jod.2020.0010.

[42] Vicky Xiuzhong Xu, Fergus Ryan, and Danielle Cave, "Mapping More of China's Tech Giants: AI and Surveillance." *Australian Strategic Policy Institute*, November 28, 2019, 18. https://doi.org/https://www.aspi.org.au/report/mapping-more-chinas-tech-giants.

information channels that support the propaganda of the CCP ideology, ensuring a cohesive form across all sectors continuing the Chinese agenda. This is the central fear across democracies: the exported use of data manipulation and coercive techniques through social media apps on democratic societies through the norms of the CCP. The mix of CCP ideology and China's technology sector creates important considerations for democratic societies using these apps, as the modern tool of influence that is not well understood.

4.3 The Case of TikTok

The case of TikTok offers a highlighted example of the future of social media as a weapon, and how it can be used to infiltrate, manipulate, and change common perceptions in a foreign society unnoticed. The TikTok algorithm is considered the most predominant example of sharp power, as it censors, controls, and manipulates information, thus creating propaganda and influence on the young audiences that interact with TikTok. TikTok will be analyzed through the theoretical framework of sharp power, including the five tenets of influence.

TikTok was created through the Chinese company ByteDance in 2016. ByteDance created two versions of this app, one for Chinese audiences called Douyin, and one to be exported to western audiences called TikTok. ByteDance acquired an American musical lyric sharing app, Musical.ly in 2018, expanding the interested clientele for TikTok and establishing the app within a younger market.[43] What sets TikTok apart from other social media apps is that it is owned by a Chinese company, while other popular apps of similar following like YouTube, Facebook, Twitter, and Instagram are owned by American companies. TikTok engages a younger crowd by offering an app function that allows users to duet other videos, creating a new output with dual video display, increasing average video engagement in ways that other apps like YouTube, or videos on Facebook, have not integrated.[44] TikTok is not just a social media app, as research has determined the hidden link between this neutral social media app and the parent company ByteDance acting as a geopolitical and ideological expansion of the CCP's agenda. The core of this argument illuminates the blurred line between Chinese government and business, and the strategic ways this impacts western actors.

[43] 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. https://doi.org/10.1108/lhtn-01-2020-0001.
[44] Ibid., 8.

The algorithm of TikTok is one of the most worrisome aspects of the social media app, as it allows for a "causal politicking" of data, as ByteDance can learn valuable information about users, including their "ease of access, lack of ideological commitment, and short cycle repetitive patterns of use".[45] Dobson et al. (2018) recognizes the intent of the algorithm to "reproduce and reaffirm normative identities" by calculating the engagement to provide a false neutral media zone for users and strategically inserting ideologies that align with the CCP.[46] The primary users are also teenagers and young adults, as 41% of users are between the ages of 16-24 and spend an average of 52 minutes per day.[47] One of the most important characteristics of TikTok's algorithm is that is location-based, allowing the algorithm to work within the local and national regulations through a seamless algorithm processing. This allows TikTok to run in over 155 countries.[48]

4.4 The Overlap of TikTok and Sharp Power: The Theoretical Analysis

The Sharp Power Rising Authoritarian Influence Report (2017) determined five main tenets of sharp power to diagnose and understand the long-term goals. The tenets include manipulation, censorship, propaganda, control, and influence. This framework adds value by defining the five key tools that are used in sharp power campaigns and helps to analyze examples of sharp power. For sharp power to be utilized, a high level of control is required by the CCP over relevant actors and national economies. Chinese firms are led by a strong government hand that determines their accessibility, profitability, and ability to export abroad.[49] The CCP relies on an infrastructure of cooperation, with mechanisms for penalties, censorship, and government promotion.[50] The integrated platform economy demonstrates China's extensive government control over civil society, impacting business decisions,

[45] Darsana Vijay, and Alex Gekker, "Playing Politics: How Sabarimala Played Out on TikTok." *The Dark Social Web: Responsibility, Manipulation, and Participation in Global Digital Spaces* 65: 717-718. Accessed June 14, 2021. https://doi.org/https://doi.org/10.1177/0002764221989769.

[46] Amy Shields Dobson, Nicholas Carah, and Brady Robards, "Digital Intimate Publics and Social Media: Towards Theorising Public Lives on Private Platforms." *Digital Intimate Publics and Social Media*, 2018, 19. https://doi.org/10.1007/978-3-319-97607-5_1.

[47] Yulun Ma, and Yue Hu, "Business Model Innovation and Experimentation in Transforming Economies: ByteDance and TikTok." *Management and Organization Review* 17, no. 2 (2021): 2. doi:10.1017/mor.2020.69.

[48] Ibid., 4.

[49] Walker and Ludwig, "Sharp Power Rising Authoritarian Influence," 21.

[50] Jian Lin, "ONE APP, TWO VERSIONS: TIKTOK AND THE PLATFORMIZATION FROM CHINA." *AoIR Selected Papers of Internet Research*, (October 5, 2020): 1. https://doi.org/10.5210/spir.v2020i0.11260.

regulation of data, and state promotion.[51] The next section will discuss TikTok actors, influence, and capacity to be a sharp tool.

4.4.1 Manipulation

The first tenet, manipulation, recognizes the overarching goal of using sharp power as a tool for power. It relies on liberal democratic norms to reach the targeted audience and offering information in a way that poisons as it is consumed.[52]

The power of the TikTok algorithm plays a steady role in its capacity to manipulate audiences. TikTok has become a tool of political engagement, as young users voice and interact with ideologies within their local TikTok algorithm. TikTok becomes a heuristic platform that ByteDance can manipulate to shift political and institutional legitimacy based on the preferences shared. This can be through targeted local initiatives and through user daily engagement that "shifts the centrality of rationality in the habermasian public sphere".[53] A recent 2019 example of TikTok manipulating information channels could be seen after the app banned 17-year-old user Feroza Aziz for creating a viral video about China's Muslim suppression. Her video slipped through the banned algorithm topics by initially acting as a makeup tutorial.[54] TikTok banning not only the video, but the account after it was discovered demonstrates the manipulation of information to exclude commentary against the CCP. The app attempts to promote a neutral multilayered information channel, however the active content moderation demonstrates otherwise. TikTok remains a vessel for highly censored messages that manipulate and shift foreign assumptions on China's actors through strategized rhetoric.

4.4.2. Censorship

Censorship as a mechanism of sharp power has implications across the potential for common action, understanding issues, and even outside actors having a more realistic view of the China the sharp power promotes.[55] The value of censorship within TikTok's algorithm flows seamlessly with manipulation, as it aims to cushion the CCP actors and agendas from foreign dissent and neutralize discussions. One of the most targeted algorithm mechanisms is

[51] Lin, "ONE APP, TWO VERSIONS: TIKTOK AND THE PLATFORMIZATION FROM CHINA," 1.
[52] Walker and Ludwig, "Sharp Power Rising Authoritarian Influence," 17-18.
[53] Vijay and Gekker, "Playing Politics: How Sabarimala Played Out on TikTok," 717.
[54] Sara Morrison, "TikTok Is Accused of Censoring Anti-Chinese Government Content, Again." Vox, November 27, 2019. https://www.vox.com/recode/2019/11/27/20985795/tiktok-censorship-china-uighur-bytedance.
[55] Walker and Ludwig, "Sharp Power Rising Authoritarian Influence," 12.

the capacity to "shadow ban", where TikTok content moderators can secretly tag a video as harmful, but do not remove the video from the app or ban the content creator. Instead, the video remains on the content creator's home page but is excluded from the local algorithm and thus has no user engagement. It is a covert method of censorship that is especially effective in democratic society, as it is almost untraceable.[56] A more specific example was discovered by The Guardian in 2019, where they revealed a study showing the CCPs control over TikTok's algorithm as the app was found censoring rhetoric by "projecting Beijing political neuroses onto the politics of other countries".[57] This was seen through the complete silencing of videos discussing the Tiananmen Square Massacre, or the genocide in Cambodia, and extended to banning criticism on institutions that can be related to the CCP's control. Tags include constitutional monarchy, separation of powers, and socialism system.[58] This has important implications as it reinforces one of the tenets of autocracies, by ensuring all information channels follow one message, even democratic information streams.

4.4.3. Propaganda

Exported propaganda supports programs, media articles, and speech to show China as a positive international influence, with values that should be replicated, admired, and the antithesis to democratic failures of inefficiency, improperly elected leaders, and less traditional values. Researchers have found a difference between propaganda based on locations, showing that it is both targeted by audience and through the message.[59] The aim of propaganda is to show the CCP's choices for strong government control over society, economy, and political ideologies that offer a more stable and reliable form of government, counteracting the work of democratic governments and showing a different portrayal of successful government.

As TikTok is a social media app, it requires a degree of stealth to input messages of propaganda within the app user engagement. Walker & Ludwig (2017) consider propaganda as the key to infiltrating and disrupting democratic institutions, as TikTok can utilize "local actors as conduits for foreign propaganda and tools of foreign manipulation", groups that are considered legitimate information sources.[60] The value of TikTok is that it incorporates many different information streams into the user content. Walker and Ludwig (2017) found that

[56] Xu, Ryan, and Cave, "Mapping More of China's Tech Giants: AI and Surveillance," 10.
[57] Ibid., 9.
[58] Ibid.
[59] Walker and Ludwig, "Sharp Power Rising Authoritarian Influence," 18.
[60] Ibid., 7.

sharp power prioritizes grass-roots democratic institutions and independent media, utilizing legitimate information channels to broadcast appropriate messages.[61] Exported propaganda includes the push by the CCP for Chinese users in politicized cities like Xinjiang, and from the Uyghur community to make videos on quality of life demonstrate one facet of the propaganda.[62] TikTok has also faced criticism as Islamic State clips have arisen of prisoners being beheaded, increasing international speculation on the power of other actors to use TikTok for propaganda.[63]

4.4.4 Control

China has the capacity to control commercial platforms across TikTok to create legitimacy, stakeholders, and regulatory institutions. The President of ByteDance, Zhang Yiming, has exemplified shifting the agendas of TikTok, the algorithm, and even the TikTok slogan to match CCP initiatives or risk critical government involvement in the company.[64] The TikTok business infrastructure itself prioritizes algorithm control, and shaded interests across foreign integration. Thus, all stakeholders must conform to the regulatory body of China's government that maintains control over user rhetoric. This ensures TikTok serves the state interests, prioritizing coordinated knowledge, culture, and religion.[65] Due to a Chinese law passed in 2017, ByteDance legally cannot share any information about the algorithm itself, making it inaccessible to all foreign actors.[66] In 2014, a whistleblower released official TikTok content moderation guidelines given to content moderators for German TikTok that provided insight into ByteDance agendas. Moderators were told to mark discourse on gender identity, sexual orientation, criticism of police and military, riots, controversial content about Putin, Trump and Kim Jong-un, and certain symbols.[67] The whistleblower handed the list to the German publication Netzpolitik, who was able to release the pivotal information to the

[61] Walker and Ludwig, "Sharp Power Rising Authoritarian Influence," 23.
[62] Rosie Perper, "Report Claims TikTok Parent Company ByteDance Is Working with China's Communist Party to Spread Propaganda on Xinjiang." Business Insider, November 29, 2019. https://www.businessinsider.com/tiktok-parent-company-bytedance-spreads-chinese-propaganda-report-2019-11.
[63] Xu, Ryan, and Cave, "Mapping More of China's Tech Giants: AI and Surveillance," 10.
[64] Zongyi Zhan, "Infrastructuralization of Tik Tok: Transformation, Power Relationships, and Platformization of Video Entertainment in China." *Media, Culture & Society* 43, no. 2 (July 21, 2020): 231. https://doi.org/10.1177/0163443720939452.
[65] Ibid., 233.
[66] Jufang Wang, "From Banning to Regulating TikTok: Addressing Concerns of National Security, Privacy, and Online Harms." *Platforms, Governance, and Global Society (PGG)* (October 20, 2020): 5. https://www.researchgate.net/publication/344584442_From_banning_to_regulating_TikTok_Addressing_concerns_of_national_security_privacy_and_online_harms.
[67] "Auszug Aus Den Moderationskriterien Von TikTok." *Netzpolitik.org*, n.d. https://cdn.netzpolitik.org/wp-upload/2019/11/tiktok-auszug-moderationsregeln-abschrift-1.pdf.

world. This list demonstrates the hidden agendas and control by the state, as the list promotes state initiatives through the TikTok algorithm itself.[68] It demonstrates the role of control influencing the content that goes to the individual phones through hidden agendas that are difficult to identify.

4.4.5 Influence

Influence creates power through consistency, and the ability for messages to be adapted to different audiences, languages, and pressures. Researchers noted that consistency is especially powerful, and almost entirely invisible when authoritarian regimes combined economic leverage with political ideology across democratic institutions.[69]

One of the most discussed concerns in foreign governments that have a strong TikTok user base is the capacity for the parent company to create incentives and penalties for users depending on their rhetoric within the app. In 2019, US Congress heard from a former TikTok employee about the power of the algorithm in creating influence through the creators it supports.[70] The Australian Strategic Policy Institute (ASPI) studied similar concerns, finding that in localized algorithm applications, certain words in specific languages and regions were silenced or banned, such as the Russian and Arabic word for "gay", "lesbian", and the Arabic word for "transgender".[71] What makes the censorship within the TikTok algorithm different from other data collection sites is that sites such as YouTube and Facebook are required to maintain global regulations that correspond with democratic values like free speech, censoring based on widely accepted norms and agendas regardless of which country the users belong to. TikTok, however, created an algorithm that moderates content through localized regulations and norms, making it moldable to conservative countries and promoting country-specific rhetoric that agrees with China's initiatives in ways that YouTube and Facebook cannot.[72] TikTok aids in cultural constructs that are consistent with the CCP, with 'traditional' norms promoted.

[68] Markus Reuter, and Chris Köver, "TikTok: Cheerfulness and Censorship." Netzpolitik.org, November 23, 2019. https://netzpolitik.org/2019/cheerfulness-and-censorship/.
[69] Walker and Ludwig, "Sharp Power Rising Authoritarian Influence," 1.
[70] Casey Newton, "TikTok Has a Credibility Problem with Congress." The Verge. The Verge, November 6, 2019. https://www.theverge.com/interface/2019/11/6/20950007/tiktok-congress-hearing-josh-hawley-censorship-china.
[71] Chris Fox, "TikTok Admits Restricting Some LGBT Hashtags." BBC News. BBC, September 10, 2020. https://www.bbc.com/news/technology-54102575.
[72] Wang, "From Banning to Regulating TikTok: Addressing Concerns of National Security, Privacy, and Online Harms," 6.

4.5 Conclusion

Sharp power tools within TikTok can only be as effective as their capacity to penetrate foreign society and influence. Questions arise as democratic governments struggle to protect domestic users, as domestic data protection and data privacy norms are attempting to meet this challenge. The next chapter aims to answer this through the case study approach.

Chapter 5: TikTok's Capacity to Infiltrate: Comparing EU and US Data Privacy Regulations

5.1 Introduction

TikTok collects information to create an engaging algorithm for individual users, which can manipulate and censor TikTok users. A study by Gil de Zuniga and Valenzuela (2011) discovered a link between political engagement via social media and overall likelihood to increase participation. When individuals are presented political ideas through media channels they follow, or trust, they are more likely to process the information with higher levels of positive association and accuracy than when they experience the same information in mass media content such as a news channel or radio. Messing and Westwood (2014) add to this argument, finding that individuals not only are more likely to trust it, but are also more likely to change their political preferences, even if it includes information they were not previously interested in. The cost-benefit analysis they go through by experiencing information via social media channels they trust increases pressure on social cues over individual ideological preferences, skewing how they internalize and trust the data for long term ideological influence.[73] The use of an algorithm to determine TikTok videos the users see creates a low-choice environment, as users do not have the power to opt-out of certain political ideas, or avoid political commentary and can be influenced through what they see. As TikTok has extensive ability to collect metadata on their users, the algorithm acts a tool of influence and requries foreign governments to understand how it can slice through information channels.

While most multinational businesses collect personally identifiable information (PII) from users for basic app functions, issues emerge as most individuals do not have the capacity to understand what their PII Is being used for, or the intent of larger app developers that are collecting the data. Thus, it creates a gap as consumers offer information for basic app functions; but in the case of TikTok, information becomes a tool of influence. Enacted legislation of the GDPR and certain US states have attempted to bridge this gap by requiring data collectors to specify what they will use the data for to increase consumer awareness, but there are still gaps in the regulations. TikTok's Privacy Policy confirms certain information that it collects, including PII information such as email, age, and information shared through content creators. At the same time, it also collects extensive location data, biometric information such as faceprints and voiceprints, and access to cookies stored in your phone

[73] Valeriani and Vaccari, "Accidental Exposure to Politics on Social Media as Online Participation Equalizer in Germany, Italy, and the United Kingdom," 1861.

even after you close the app.[74] These create a wide metadata of information with additional implications for all users, especially younger ones under the age of 18.

5.2 Analyzing the GDPR

The EU passed the General Data Protection Regulation (GDPR) in 2017. It is an extensive regulatory body that includes several articles for individual-led data privacy standards. Seven of which are relevant for TikTok users. Article 5(1) includes the first three principles, Purpose Specification, Data Minimization, and Transparency. These ensure the consumer is aware of exactly what data is collected, how long it will be stored, if it will be used for research purposes, and long-term guarantees that the data collected is only used in the legal ways defined at the initial user agreement.[75] Article 7(2) of the GDPR ensures that consumers are provided this information in clear, understandable communication. This shifts previous industry standards that provided the entire privacy statement and usage of data in a long, incomprehensible, and technical verbiage that made it difficult for the average user to understand what data privacy rights they are agreeing to.[76] A secondary issue that GDPR targeted was the binary yes/no approach to data rights. Consumers either had to agree to all the terms, or not use the good or service. Article 7(3) recognizes this, requiring companies to break down permissions that impact consent, so they can agree to some and not all, and withdraw at any time.[77] The last two articles create regulations for companies that hold the data, to include Data Protection by Design (Article 15-2), and Data Protection Impact Assessment (Article 35-1). These require businesses to have protectionary data measures as described above from when they first enter data, to the end of data processing. To regulate this, businesses must perform assessments on their data usage to recognize the potential danger to consumers, including risks, legitimate interest of data controllers, the necessity of the data collection, and safeguards to protect users.[78]

The GDPR creates bottom-up level governance across the EU by providing individuals the capacity and accessibility to regulate and consent to data collection, analysis, and usage by third-party controllers. Some critics argue that this creates problems, as the GDPR provides individuals data rights, but many do not have the interest, knowledge, or

[74] "Privacy Policy." TikTok. Accessed June 16, 2021. https://www.tiktok.com/legal/privacy-policy?lang=en#section-1.
[75] Nurul Momen, Majid Hatamian, and Lothar Fritsch, "Did App Privacy Improve After the GDPR?" *IEEE Security & Privacy* 17, no. 6 (2019): 13. https://doi.org/10.1109/msec.2019.2938445.
[76] Ibid., 14.
[77] Ibid.
[78] Ibid., 13.

ability to properly understand how multinational firms are using their data on a day-to-day basis or the large-scale impact of the information they provide. It is assuming too much of the average individual to put the larger security risks of metadata on the individual to self-regulate.[79]

Other arguments against the GDPR say that the high fixed costs businesses accrue to match data protection standards cut out small businesses from competing, and thus create a reliance on big data firms like Google, increasing sectoral industry control. Additionally, competitors in the US view the GDPR as a violation of free speech, hurting the norm-making credibility the GDPR offers on the global scale.[80]

5.2.1 Can the GDPR Protect Users from Harmful TikTok Influence?

The GDPR offers two main protections for EU users, a normative defense, and a technical infrastructure. It created widely acknowledged data privacy norms that multinational business must adhere to, thus exporting these norms to other regions. Each TikTok conflict that is brought to the EU creates a normative precedence that prioritizes consumer interests through regulatory and legal mechanisms.

The GDPR offers technical protection for users against foreign influence through the extensive self-regulated data privacy standards and improving accessible knowledge for average consumers. A study by Karlstad University (2019) found that after the GDPR was adopted, user consent shifted to match the data minimization principle. Users saw significant improvement in providing consent for different types of data requested by apps, and increased accountability for companies that failed to properly clarify how they used the data and their interests. However, the study also found that the data collection methods shifted to be more covert, and businesses began asking for less permissions. However, apps also began requesting more invasive permissions like sensory ones, including access to camera, microphone, and body sensors in lieu of previous data collection methods.[81] Apps shifted to relying on location-triggered advertisements, using sensor access that includes conditional access to location, contacts, and motion.[82] This put consumers at a new disadvantage, as they

[79] Sylvie Delacroix, and Neil D Lawrence, "Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance." *International Data Privacy Law*, (October 12, 2018), 238. https://doi.org/10.1093/idpl/ipz014.

[80] Roslyn Layton, and Silvia Elaluf-Calderwood, "A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices." *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*, November 2019, 2. https://doi.org/10.1109/cmi48017.2019.8962288.

[81] Momen, Hatamian, and Fritsch, "Did App Privacy Improve After the GDPR," 17-18.

[82] Ibid., 1.

could properly control and understand data requests from apps, however companies adapted data collection methods that were equally as concerning and invasive.

The GDPR has had multiple conflicts with TikTok over the lack of consumer data control, and the invasive data collection techniques that have emerged about the TikTok app. These conflicts test the power of the GDPR as a regulatory institution with the capacity to protect national data interests.

One conflict arose as global governments, including the EU, cited concerns over TikTok user data being processed in foreign data processing plants. TikTok then agreed to store EU user data in an Irish data processing center, thus enabling Ireland to have data jurisdiction over all data disputes and diminishing the accessibility of data by foreign actors like the CCP.[83] This set an important precedent by recognizing the potential for manipulation by foreign owned governments as soon as data leaves national jurisdiction.[84]

TikTok also faced incomplete data protection standards for minors in a 2017 case. Brought by the former Children's Commissioner for England, a legal action lawsuit was filed against TikTok for collecting excessive amounts of minors' data via "shadowy collection practices" and failing to provide parents the right to know what information is being collected.[85]

The most recent GDPR review of TikTok includes the February 2021 lawsuit filed by Bureau Européen des Unions de Consommateurs (BEUC) about TikTok's shady information collection practices. BEUC argues that TikTok is not adhering to the privacy principles of the GDPR, as the data processing described in TikTok's Terms of Service are unfair, misleading, and harm children that are unable to recognize "hidden advertising and potentially harmful content on its platform".[86] A German journalist, Matthias Eberl, released a similar report in 2019 after invasive data collection methods were found through the TikTok app, specifically canvas fingerprinting. He describes this as "a fingerprinting technique in which the website

[83] Leo Kelion, "TikTok to Open $500m Data Centre in Ireland." BBC News. BBC, August 5, 2020. https://www.bbc.com/news/technology-53664997.

[84] Emmanuel Pernot-Leplay, "EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?," Colorado Technology Law Journal 18, no. 1 (2020): 28.

[85] "TikTok Sued for Billions over Use of Children's Data." BBC News. BBC, April 21, 2021. https://www.bbc.com/news/technology-56815480.

[86] "BEUC Files Complaint against TikTok for Multiple EU Consumer Law Breaches." BEUC, February 16, 2021. https://www.beuc.eu/publications/beuc-files-complaint-against-tiktok-multiple-eu-consumer-law-breaches/html.

asks the browser to draw a hidden image and using that unique image to identify the browser version, operating system, and other information regarding the execution environment".[87]

Additionally, the GDPR constructed new communication networks that still rely on almost all Chinese hardware manufacturers like Huawei, ZTE and Lenovo. These companies are under similar business expectations as TikTok's parent company ByteDance, so the interests of the CCP are integrated within the GDPR channels itself. Technology experts warn national leaders that using Chinese vendors has implications for possible backdoors into the EUs data, cloud network, and other covert methods.[88]

The GDPR is successful in offering users stronger data control, especially with minors, however the capacity for foreign influence through data is not necessarily nulled. The concerns over the TikTok algorithm itself, including the capacity for censorship, manipulation, and corrupting information channels is still legally acceptable under the GDPR. The GDPR has a strong hand in protecting data collecting and processing, however the ambiguity over TikTok's algorithm, the interconnected CCP and ByteDance agendas, and the potential backdoors that increase China's capacity for covert data collection leave large gaps that the GDPR must navigate in the upcoming years.

5.3 US Data Protection Mechanisms

US data protection regulations are much more patchworked than the GDPR, with sectoral federal laws and more comprehensive state laws. The regulations are divided into three sections, including the oversight of the Federal Trade Commission, varying federal sectoral laws, and state laws. The US is considered a highly minimalist approach to data governance, preferring industry-led norms, and considering extensive data protection a restriction on the Constitutional First Amendment, freedom of expression.[89]

The Federal Trade Commission (FTC) is the highest national privacy authority in the US, covering competition, consumer protection, and privacy. The FTC is the main federal legal mechanism for protecting data protection by overseeing data privacy cases and creating incentives for businesses to follow fair trade laws.[90] The FTC Act (1914) allows the FTC to

[87] Pellaeon Lin, "TikTok vs Douyin: A Security and Privacy Analysis." The Citizen Lab, March 22, 2021. https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/.

[88] Layton and Elaluf-Calderwood, "A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices," 3-4.

[89] Pernot-Leplay, "EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?," 35.

[90] David A. Hyman, and William E. Kovacic, "Implementing Privacy Policy: Who Should Do What?" *SSRN Electronic Journal*, February 2018, 12. https://doi.org/10.2139/ssrn.3123115.

pursue data protection breaches that include "unfair or deceptive acts or practices in or affecting commerce".[91] Rather than utilizing fines as the main disincentive for dangerous privacy policies like the GDPR, the FTC instead attempts a consent order and then official litigation against the business in question.[92] The FTC also organizes national conferences discussing the latest concerns to data privacy, and connecting government agencies, businesses, and NGOs that create national level data 'common law', making it an important data norm-setting institution. However, the FTC is viewed as a very broad mechanism for accountability in data privacy, as it does not have rulemaking authority and narrow enforcement guidelines.[93]

Another US regulatory body is the Committee on Foreign Investment in the United States (CFIUS). This group analyzes business merges and acquisitions, transactions, and foreign investment into US companies to analyze foreign actors' intent.[94] Under former President Trump, CFIUS merged with another accountability body, the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) that analyzes the "economic and security impact of foreign investments in emerging technologies in the United States". Entering the start of 2020, CFIUS now has the accountability function to analyze China's investments into entrepreneurial buyouts across the US.[95] This is relevant as China invests in American technology start-ups, financial institutions, and infrastructure across the US creating security risks that CFIUS has the legitimacy to review.

The US federal data privacy regulations also have sectoral laws that protect certain vulnerable groups from privacy violations. The only relevant law to TikTok is the Children's Online Privacy Protection Act of 1998 (COPPA), which specifically protects the privacy of children and requires parental consent for all minors under 13 that may provide personal information to companies. It is important as it defines data misuse in this case of minors and regulates how companies can collect data to provide legal accountability for the vulnerable user community. Children have much greater data privacy protection, and institutionalized

[91] Shaun G. Jamison, "Creating a National Data Privacy Law for the United States." *Cybaris*, 2, 10, no. 1 (2019): 7. https://open.mitchellhamline.edu/cybaris/vol10/iss1/2.
[92] Ibid., 8.
[93] Hyman, and Kovacic, "Implementing Privacy Policy: Who Should Do What?," 14.
[94] The Committee on Foreign Investment in the United States (CFIUS). Accessed June 12, 2021. https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.
[95] Anat Alon-Beck, "TikTok, Your Time Is Up." Forbes, December 8, 2020. https://www.forbes.com/sites/anatalonbeck/2020/12/08/tiktok-your-time-is-up/.

norms, however, still require individual "voluntary self-regulation".[96] Federal laws assume individuals and legal guardians must safeguard and protect their own data, and that "privacy harms are measured by their impact on the individual".[97]

State level data protection laws are much more comprehensive and consumer-oriented, as 50 states now have some form of data protection law.[98] The priorities vary from state to state, from focusing on company-level regulation, state-wide lists that protect residents from privacy scandals, and regulations providing rights to individuals under the same logic as the GDPR.

The most notable state regulation is the California Consumer Privacy Act of 2018 (CCPA). The CCPA is the most extensive data protection regulation passed in the US to date and has many parallels with the GDPR. It includes protections for individual data sharing consent, including information about what is collected, if the data will be sold and accessible to other parties, and provide individuals the right to request their data not be sold, and full deletion.[99] It includes similar definitions of PII, defining personal information through its relations and linkage to individual or household consumers.[100] California is important as an example of data privacy regulations within US national infrastructure, enforcing strong business codes and acting as the de facto national law as other states follow this lead.[101]

The US faces criticism as the patchwork laws increase business compliance costs as they must invest recourses to ensure they meet all state level laws.[102] Additionally, there is not a widely recognized definition in the US for PII, making it difficult for individuals to take companies that exploit their data to court through legal precedence and business law. Consumers are required to have extensive recourses and knowledge about burden of proof legislation to take any data privacy issues through accountability measures. They face both constitutional limitations through freedom of speech legislation, and FTC limits within established common law privacy rights.[103]

---

[96] Pernot-Leplay, "EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?," 37.
[97] Alice E. Marwick and Danah Boyd, "Networked Privacy: How Teenagers Negotiate Context in Social Media." *New Media & Society* 16, no. 7 (2014): 1053. https://doi.org/10.1177/1461444814543995.
[98] Jamison, "Creating a National Data Privacy Law for the United States," 12.
[99] Ibid.,13.
[100] Pernot-Leplay, "EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?," 42.
[101] Jamison, "Creating a National Data Privacy Law for the United States," 13-14.
[102] Ibid., 18.
[103] Ibid., 15.

5.3.1 Can the US Regulations Protect Users from Harmful TikTok Influence?

In comparison to the GDPR, the regulatory protection for American TikTok users is much more self-regulated and inaccessible for the average user to properly protect their identity as an online consumer. Even with the regulatory power of the FTC and CFIUS to hold companies accountable, there is still a weak data protection infrastructure that leaves most consumers at risk to TikTok influence. Users are vulnerable in a position that TikTok can readily access American information streams and shift perspectives across the average user.

The Federal Trade Commission first investigated TikTok in 2019 as a claim arose from the Department of Justice that TikTok failed to provide the required COPPA data privacy steps for minors using the app. The FTC found that TikTok "failed to seek parental consent before collecting names, email addresses, and other personal information from users under the age of 13".[104] The FTC fined TikTok $5.7 million for the privacy breach, the largest fine ever given under COPPA.[105] Recently, in 2020, a Massachusetts tech policy group went to the FTC arguing that TikTok failed to properly delete the videos and personal information of the users that were victims in the original investigation.[106]

TikTok also received a large amount of pressure from the Trump administration (2017-2021), as both former President Trump and Vice President Mike Pence have publicly announced their distrust for TikTok, promising to use their political capital to investigate the app and hopefully ban it from US audiences.[107] Some argue that the lack of a federal data privacy infrastructure led to the Trump Administration relying on other avenues of securitization, such as Trump signing an Executive Order, and the Senate passing a bill to ban TikTok on all government devices.[108] Concerns over TikTok were removed from the data privacy field and shifted to concerns over national security and American interests. Trump and his administration coupled with the CFIUS to investigate the intent of Chinese actors

[104] Federal Trade Commission, Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law § (2019). https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.

[105] BBC News, "TikTok Sued for Billions over Use of Children's Data,".

[106] Diane Bartz, "US Government Is Investigating TikTok for Failing to Change How It Collects Children's Personal Information Following Last Year's $5.7 Million Privacy Fine." Business Insider. Business Insider, July 8, 2020. https://www.businessinsider.com/exclusive-us-probing-allegations-tiktok-violated-childrens-privacy-sources-2020-7.

[107] Zak Doffman, "Warning-Apple Suddenly Catches TikTok Secretly Spying On Millions Of iPhone Users." Forbes, June 27, 2020. https://www.forbes.com/sites/zakdoffman/2020/06/26/warning-apple-suddenly-catches-tiktok-secretly-spying-on-millions-of-iphone-users/?sh=5e53531f34ef.

[108] "Hawley's Bill to Ban TikTok on Government Devices Passes Senate Unanimously." Senator Josh Hawley, August 6, 2020. https://www.hawley.senate.gov/hawleys-bill-ban-tiktok-government-devices-passes-senate-unanimously.

through the ByteDance purchase of the US company Musical.y. The CFIUS investigation shifted global perceptions of TikTok as a neutral actor. TikTok was accused of threatening national security, with major implications as the American user base was high. The CFIUS used this report to attempt to force TikTok to merge with US companies, under the premise of protecting US users and merging TikTok intents with American influence.[109]

Principles that form the core of the GDPR, such as data minimization and transparency do not exist under federal data privacy regulations, so consumers are again at a legal disadvantage for rights.[110] TikTok faced similar backlash by US users requiring the company to again shift domestic data from foreign data processing plants to two trusted data servers in Virginia, and Singapore, showing that even without the extensive data accountability of the GDPR, TikTok falls to domestic pressures amid security scandals.[111] Even so, the FTC continues to rely on NGOs for policy implementation and bringing cases to federal level jurisdiction.[112] This demonstrates holes in the FTC's capacity to hold TikTok accountable, as it requires additional third-party awareness for the FTC to consider the case.

Another major challenge for data privacy misuse rests in the lack of a common definition for what constitutes a data privacy right. This can be seen through the common argument across US policymakers that controlling data privacy, in the way that the GDPR does, is a restriction of the US First Amendment, as it blocks freedom of expression. Researchers from the Center for Strategic International Studies (2020) argues that this norm can be traced to the Cambridge Analytical scandal with Facebook, where user information was also exploited for political purposes.[113] Social media sites have full capacity to police their sites for information they want to block, however this norm becomes complicated as anti-democracy foreign actors are added to the mix. The US regulatory system for data privacy is stuck in a spiral of attempting to protect American users from malicious activity

[109] William Alan Reinsch, Patrick Saumell, Isabella Frymoyer, and Jack Caporal, "TikTok Is Running out of Time: Understanding the CFIUS Decision and Its Implications." TikTok Is Running out of Time: Understanding the CFIUS Decision and Its Implications | Center for Strategic and International Studies, September 2, 2020. https://www.csis.org/analysis/tiktok-running-out-time-understanding-cfius-decision-and-its-implications.

[110] Pernot-Leplay, "EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?," 3.

[111] Reinsch, Saumell, Frymoyer, Jack Caporal, "TikTok Is Running out of Time: Understanding the CFIUS Decision and Its Implications,".

[112] Associated Press, "TikTok Is Violating Children's Privacy, Advocacy Groups Warn." NBCNews.com. NBCUniversal News Group, May 15, 2020. https://www.nbcnews.com/tech/security/tiktok-violating-children-s-privacy-advocacy-groups-warn-n1207716.

[113] Reinsch, Saumell, Frymoyer, and Caporal, "TikTok Is Running out of Time: Understanding the CFIUS Decision and Its Implications,".

online and harmful foreign influence, while also relying on a highly passive data environment where users police their own behavior.

In 2020, additional concerns emerged as two trusted american companies launched independent investigations into TikTok data collection and user privacy laws. The Wall Street Journal released an article alleging that TikTok had used invasive techniques that "skirted a privacy safeguard in Google's Android operating system to collect unique identifiers from millions of mobile devices, data that allows the app to track users online without allowing them to opt out".[114] Apple also discovered in June 2020 that TikTok was secretly accessing users clipboard notes that show what the user has recently copied.[115] The FTC responded through a large overhaul of popular social media apps, requiring that a list of social media apps with similar allegations release information showing how they collect data via algorithms and codes, how it is used for ad content, algorithms tied to personal information, and their practices for minors using the social media sites. This list includes Amazon.com, ByteDance Ltd, Facebook, Reddit, Twitter, Snap and YouTube.[116] ByteDance legally was not permitted to provide the TikTok algorithm under the aforementioned national Chinese law, prohibiting the share of technological algorithms or related information to foreign actors.

The state level regulations have provided signifigantly more user protection and quick accountability. In 2020, a lawsuit was filed under the Illinois BIPA Act (2008) that protects users from biometric identification within apps, including facial recognition, fingerprints, or voiceprint. The lawsuit argues TikTok failed to acquire parental consent for minors and collected facial recognition scans. It also alleges that TikTok is unwilling to provide information on how the facial scans data are used, and how long they are held.[117]

TikTok is highly scrutinized for their data collection and the potential to weaponize it, however this is viewed through its capacity for influence rather than through the lens of data collection itself. While the data localization is a strong step towards protecting user data

[114] Kevin Poulsen, and Robert McMillan, "WSJ News Exclusive | TikTok Tracked User Data Using Tactic Banned by Google." The Wall Street Journal. Dow Jones & Company, August 11, 2020. https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738?mod=article_inline.

[115] Doffman, "Warning-Apple Suddenly Catches TikTok Secretly Spying On Millions Of IPhone Users,".

[116] Federal Trade Commission, FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information § (2020). https://www.ftc.gov/news-events/press-releases/2020/12/ftc-issues-orders-nine-social-media-video-streaming-services.

[117] Bess Hinson, Ashley Thomas, and Bisi Adeyemo, "Lessons from TikTok: Federal and State Law Implications for Children's Biometric Data Privacy: Biometric Update." Biometric Update, November 25, 2020. https://www.biometricupdate.com/202011/lessons-from-tiktok-federal-and-state-law-implications-for-childrens-biometric-data-privacy.

within influence campaigns and protecting the rights of users, the federal and state infrastructures have not shown the capability of holding TikTok accountable without additional legislation being passed.

Chapter 6: Key Findings

6.1 Key Findings

The role of nationalized norms for data sovereignty rights and consumer protection creates a global environment that harmful foreign actors can infiltrate as democratic governments face an externality problem of data. Global concerns over data weaponization have demonstrated that the definition of data sovereignty is still unclear in who it protects. The literature on sharp power was relevant in examining the main research question, "What are the implications of the popular social media app TikTok being used as a vector of foreign influence on individual users in democratic societies?" The theoretical foundation for sharp power aided in this approach, as recent literature has discussed sharp power as a tool of influence and implications for democracies. The case study approach of the thesis, leading into the secondary research question "How do the current democratic institutions protecting data privacy laws protect users from the influence of sharp power through the Chinese social media app TikTok?" identified how democracies can properly protect their societies from sharp power as a weapon of influence. The look at the US and EU data governance structures provides a first look at modern infrastructure with an even more recent tool, moving past the established sharp power literature to understand implications for two different governance regimes themselves. The analysis has demonstrated that the GDPR is effectively a user-based protection scheme, while the US is a market-based protection scheme. Should the EU and US data governance structures be unable to adapt, we can expect the current power of data sovereignty to shift.

The GDPR demonstrates the integral value of an accountability structure. It offers a normative definition of data privacy that powers other data privacy regimes and encourages individuals to understand the danger and weaponization of data they provide to companies. The GDPR is a strong barrier to China's efforts of collecting and manipulating data to their own agendas. However, it still has major security gaps as its users are vulnerable through the TikTok algorithm itself, as the app has continued to show signs of censorship, propaganda, influence, and ultimately coercion. The GDPR is effective as a regional data privacy regime but fails as their accountability cannot be exported to foreign owned businesses without a global data governance institution. Both the lack of a global definition for PII, and the inability to examine the TikTok algorithm, the power of GDPR in the case of ByteDance is diminished. The GDPR has important future implications if the governance regime is unable to adapt to modern technology shifts; the accountability function but must adapt its definitions and business regulations to protect users from new technology breaches.

The US data privacy governance also demonstrates glaring holes that make most users across the US incredibly vulnerable. The US fails as a norm-setting institution as the data governance regime is both inadequate across current data concerns and lacks an accountability framework. Daily internet users across the US have demonstrate increased concerns as a result. A 2019 Pew Poll found that 63% of Americans reported knowing "little or nothing at all" about national data privacy regulations, and actions they can take for self-regulation.[118] NGOs are the closest accountability institution in the US, and individuals are left with narrow channels of data privacy law to self-regulate. While the FTC has grown in their role as the key litigation tool for accountability, it is still weak and fails to properly punish businesses that violate common law guidelines. Americans are faced with important implications if they are unable to access data privacy accountability mechanisms via state, or national level governance structures. As the national level lawmaking is unable to move out of sectoral data privacy agenda setting, the states become wardens of privacy to pass legal definitions for state privacy, burden of harm after privacy breaches, and accountability bodies.

The key findings of this study demonstrate the need for modern defense mechanisms against an invisible, individualized weapon. The lack of a global data privacy hinders the power of domestic governments to protect users from foreign actors' capacity to weaponize data, infiltrate democratic institutions and shift trusted information channels. With the current nationalization of technology sector accountability and agenda-setting, each country is vulnerable to weaponization of social media against their own societies. The lack of global consent to define how large companies can use data and for which purposes create ethical and legal barriers, and the case of TikTok is not isolated. Other recent examples include the 2016 Cambridge Analytica scandal where Facebook, a US technology company, was a tool of influence by Russian actors to manipulate and coerce users during the US Presidential Election, and cases of Huawei stealing African Union headquarters data for five years in Malta from 2012-2017.[119] TikTok is a topical politicized issue in today's social media discussions, but it is not alone in demonstrating the security risks of lax data privacy norms and only demonstrates how necessary improved governance structures are. The analysis of

[118] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." *Pew Research Center*, November 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[119] Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," 6, 22.

power relationships remains tricky as they are both westernized and rooted in democratic values, making it important to understand how power relationships withstand pressure from non-western values. There is still uncertainty in the results as sharp power is still such a new theoretical tool of influence. The research used in this analysis is almost exclusively from the western gaze and has not developed feedback across the academic sector. Additional uncertainly lies in the inability to examine the TikTok algorithm itself, as researchers assume it provides the most startling example of sharp power by revealing both foreign agendas, and the power of infiltration through data. It would add significant value to future studies of TikTok, sharp power, and protection through data privacy regimes to understand how the algorithm targets and infiltrates based on data collection. Additional research into sharp power as a modern power relationship theory. Additional case studies covering different examples of democratic governments and varying data privacy norms would add value to the existing definition of sharp power by offering a more applicable definition to democracies outside of the west. Research would need to consider important implications such as trust in information channels found across social media, the conception of democratic values within social media, and the role of personal initiative in data governance.

6.2 Policy Recommendations

6.2.1 European Union Recommendations

1. The GDPR is effective in holding the technology sector accountable but must pivot its current initiatives and definitions of data sovereignty to better meet modern demands. The GDPR may protect users by requiring apps to share the individual data collection methods, however it leaves backdoor traps as businesses switched to conditional data requests. The GDPR must integrate flexible legislation to cover new tools of data collection as they arise, to ensure it carries protection across all apps and user interface.

6.2.2 United States Recommendations

1. US policymakers have two policy areas that must be amended to match current data protection needs. The first is a nationally accepted PII definition, to allow national legal jurisprudence and state level initiatives under data privacy legislation. A definition for general data rights is necessary for an accountability body to have influence among US and foreign owned businesses that collect data. Businesses would have lower fixed costs as the data privacy laws they must adhere to are nationalized, rather than the current state

by state basis. It would also increase overall user awareness as their rights become congruent from state to state.

6.2.3 General Recommendations

1. It is imperative for national governments form an established definition of data privacy to initiate rule-based norm making in all exported data companies. Governments must be able to identify who is collecting data, what they are collecting, and the intents of actors that have access to it. The governance regime must prioritize creating a legal barrier and consequences to businesses that stray from their stated intents and actions as agreed upon by the individual user. National governance institutions must also remain flexible to adapt to significant technology changes. Questions remain as important questions about global data privacy jurisdiction, exported policy making, and inadequate cross-border governance structures are left unanswered, as domestic legislation is unable to penetrate the global periphery.

References

"Auszug Aus Den Moderationskriterien Von TikTok." *Netzpolitik.org*, n.d. https://cdn.netzpolitik.org/wp-upload/2019/11/tiktok-auszug-moderationsregeln-abschrift-1.pdf.

"BEUC Files Complaint against TikTok for Multiple EU Consumer Law Breaches." *BEUC*, February 16, 2021. https://www.beuc.eu/publications/beuc-files-complaint-against-tiktok-multiple-eu-consumer-law-breaches/html.

"Hawley's Bill to Ban TikTok on Government Devices Passes Senate Unanimously." *Senator Josh Hawley*, August 6, 2020. https://www.hawley.senate.gov/hawleys-bill-ban-tiktok-government-devices-passes-senate-unanimously.

"Privacy Policy." *TikTok*. Accessed June 16, 2021. https://www.tiktok.com/legal/privacy-policy?lang=en#section-1.

"TikTok Sued for Billions over Use of Children's Data." *BBC News*, April 21, 2021. https://www.bbc.com/news/technology-56815480.

Alon-Beck, Anat. "TikTok, Your Time Is Up." *Forbes*, December 8, 2020. https://www.forbes.com/sites/anatalonbeck/2020/12/08/tiktok-your-time-is-up/.

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. https://doi.org/10.1108/lhtn-01-2020-0001.

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." *Pew Research Center*, November 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Bartz, Diane. "US Government Is Investigating TikTok for Failing to Change How It Collects Children's Personal Information Following Last Year's $5.7 Million Privacy Fine." *Business Insider*, July 8, 2020. https://www.businessinsider.com/exclusive-us-probing-allegations-tiktok-violated-childrens-privacy-sources-2020-7.

Beeson, Mark, and Shaomin Xu. "Leadership with Chinese Characteristics: What Role for Soft Power?" *Global and Regional Leadership of BRICS Countries*, 2016, 169–88. https://doi.org/10.1007/978-3-319-22972-0_10.

Biersteker, Thomas. "The Potential of Europe's Sharp and Soft Power." *Global Policy* 11, no. 3 (May 18, 2020): 384–87. https://doi.org/10.1111/1758-5899.12815.

Cole, J. Michael. "THE HARD EDGE OF SHARP POWER: Understanding China's Influence Operations Abroad," October 2018, 1–36. https://macdonaldlaurier.ca/files/pdf/20181022_MLI_China's_Influence_(Cole)_PAPER_WebreadyF.pdf.

Delacroix, Sylvie, and Neil D Lawrence. "Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance." *International Data Privacy Law*, October 12, 2018, 1–43. https://doi.org/10.1093/idpl/ipz014.

Dobson, Amy Shields, Nicholas Carah, and Brady Robards. "Digital Intimate Publics and Social Media: Towards Theorising Public Lives on Private Platforms." *Digital Intimate Publics and Social Media*, 2018, 3–27. https://doi.org/10.1007/978-3-319-97607-5_1.

Doffman, Zak. "Warning-Apple Suddenly Catches TikTok Secretly Spying On Millions Of IPhone Users." *Forbes*, June 27, 2020. https://www.forbes.com/sites/zakdoffman/2020/06/26/warning-apple-suddenly-catches-tiktok-secretly-spying-on-millions-of-iphone-users/?sh=5e53531f34ef.

Dowding, Keith. “Why Should We Care about the Definition of Power?” *Journal of Political Power* 5, no. 1 (2012): 119–35. https://doi.org/10.1080/2158379x.2012.661917.
Federal Trade Commission, Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children’s Privacy Law § (2019). https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc.
Floridi, Luciano. “The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU.” *SSRN Electronic Journal*, August 12, 2020, 369–78. https://doi.org/https://doi.org/10.1007/s13347-020-00423-6.
Fox, Chris. “TikTok Admits Restricting Some LGBT Hashtags.” *BBC News*, September 10, 2020. https://www.bbc.com/news/technology-54102575.
FTC Issues Orders to Nine Social Media and Video Streaming Services Seeking Data About How They Collect, Use, and Present Information § (2020). https://www.ftc.gov/news-events/press-releases/2020/12/ftc-issues-orders-nine-social-media-video-streaming-services.
Hinson, Bess, Ashley Thomas, and Bisi Adeyemo. “Lessons from TikTok: Federal and State Law Implications for Children's Biometric Data Privacy: Biometric Update.” Biometric Update, November 25, 2020. https://www.biometricupdate.com/202011/lessons-from-tiktok-federal-and-state-law-implications-for-childrens-biometric-data-privacy.
Hoffman, Samantha. “Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion.” *Australian Strategic Policy Institute* 21 (October 2019): 1–34. https://doi.org/https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.
Hyman, David A., and William E. Kovacic. “Implementing Privacy Policy: Who Should Do What?” *SSRN Electronic Journal*, February 2018, 1–28. https://doi.org/10.2139/ssrn.3123115.
Iqbal, Mansoor. “TikTok Revenue and Usage Statistics (2021).” Business of Apps, July 2, 2021. https://www.businessofapps.com/data/tik-tok-statistics/.
Jamison, Shaun G. “Creating a National Data Privacy Law for the United States.” *Cybaris*, 2, 10, no. 1 (2019): 1–41. https://open.mitchellhamline.edu/cybaris/vol10/iss1/2.
Kelion, Leo. “TikTok to Open $500m Data Centre in Ireland.” *BBC News*, August 5, 2020. https://www.bbc.com/news/technology-53664997.
Layton, Roslyn, and Silvia Elaluf-Calderwood. “A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices.” *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*, November 2019, 1–7. https://doi.org/10.1109/cmi48017.2019.8962288.
Levy, Jack S. “Case Studies: Types, Designs, and Logics of Inference.” *Conflict Management and Peace Science* 25, no. 1 (March 1, 2008): 1–18. https://doi.org/10.1080/07388940701860318.
Li, Minghao, Wendong Zhang, and Chad Hart. "What Have We Learned from China’s Past Trade Retaliation Strategies?" *Choices* 33, no. 2 (2018): 4. Accessed July 27, 2020. www.jstor.org/stable/26487436.
Lin, Jian. “ONE APP, TWO VERSIONS: TIKTOK AND THE PLATFORMIZATION FROM CHINA.” *AoIR Selected Papers of Internet Research*, October 5, 2020. https://doi.org/10.5210/spir.v2020i0.11260.
Lin, Pellaeon. “TikTok vs Douyin: A Security and Privacy Analysis.” The Citizen Lab, March 22, 2021. https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/.

Liu, Lizhi. “The Rise of Data Politics: Digital China and the World.” *Studies in Comparative International Development*56, no. 1 (March 19, 2021): 45–67. https://doi.org/10.1007/s12116-021-09319-8.

Ma, Yulun, and Yue Hu. “Business Model Innovation and Experimentation in Transforming Economies: ByteDance and TikTok.” *Management and Organization Review* 17, no. 2 (2021): 1-7. doi:10.1017/mor.2020.69.

Manancourt, Vincent. “Why Europe's Hands Are Tied on TikTok.” *POLITICO*, September 9, 2020. https://www.politico.eu/article/tiktok-europe-privacy-gdpr-complexity-ties-hands/.

Marwick, Alice E, and Danah Boyd. “Networked Privacy: How Teenagers Negotiate Context in Social Media.” *New Media & Society* 16, no. 7 (2014): 1051–67. https://doi.org/10.1177/1461444814543995.

Momen, Nurul, Majid Hatamian, and Lothar Fritsch. “Did App Privacy Improve After the GDPR?” *IEEE Security & Privacy* 17, no. 6 (2019): 10–20. https://doi.org/10.1109/msec.2019.2938445.

Morrison, Sara. “TikTok Is Accused of Censoring Anti-Chinese Government Content, Again.” *Vox*, November 27, 2019. https://www.vox.com/recode/2019/11/27/20985795/tiktok-censorship-china-uighur-bytedance.

Newton, Casey. “TikTok Has a Credibility Problem with Congress.” *The Verge*, November 6, 2019. https://www.theverge.com/interface/2019/11/6/20950007/tiktok-congress-hearing-josh-hawley-censorship-china.

Noori, Maral, Daniel Jasper, and Jason Tower. Report. *US Institute of Peace*, 2015. Accessed July 8, 2021. http://www.jstor.org/stable/resrep20190.

Nye, Joseph S. "Public Diplomacy and Soft Power." *The Annals of the American Academy of Political and Social Science* 616 (2008): 94-109. Accessed July 8, 2021. http://www.jstor.org/stable/25097996.

Pernot-Leplay, Emmanuel. "EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?," *Colorado Technology Law Journal* 18, no. 1 (2020): 25-48.

Perper, Rosie. “Report Claims TikTok Parent Company ByteDance Is Working with China's Communist Party to Spread Propaganda on Xinjiang.” *Business Insider*, November 29, 2019. https://www.businessinsider.com/tiktok-parent-company-bytedance-spreads-chinese-propaganda-report-2019-11.

Poulsen, Kevin, and Robert McMillan. “WSJ News Exclusive | TikTok Tracked User Data Using Tactic Banned by Google.” *The Wall Street Journal*. Dow Jones & Company, August 11, 2020. https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738?mod=article_inline.

Press, Associated. “TikTok Is Violating Children's Privacy, Advocacy Groups Warn.” *NBCNews.com*. NBCUniversal News Group, May 15, 2020. https://www.nbcnews.com/tech/security/tiktok-violating-children-s-privacy-advocacy-groups-warn-n1207716.

Reinsch, William Alan, Patrick Saumell, Isabella Frymoyer, and Jack Caporal. “TikTok Is Running out of Time: Understanding the CFIUS Decision and Its Implications.” TikTok Is Running out of Time: Understanding the CFIUS Decision and Its Implications | *Center for Strategic and International Studies*, September 2, 2020. https://www.csis.org/analysis/tiktok-running-out-time-understanding-cfius-decision-and-its-implications.

Reuter, Markus, and Chris Köver. “TikTok: Cheerfulness and Censorship.” *Netzpolitik.org*, November 23, 2019. https://netzpolitik.org/2019/cheerfulness-and-censorship/.

Schneider, Ingrid. “Democratic Governance of Digital Platforms and Artificial Intelligence?” *JeDEM - eJournal of eDemocracy and Open Government* 12, no. 1 (July 2020): 1–24. https://doi.org/10.29379/jedem.v12i1.604.

Seawright, Jason, and John Gerring. “Case Selection Techniques in Case Study Research.” *Political Research Quarterly*61, no. 2 (June 2008): 294–308. https://doi.org/10.1177/1065912907313077.

Shao, Jingkai. “Exploring China’s‘ Sharp Power’: Conceptual Deficiencies and Alternati.” *Transcommunication* 6, no. 2 (September 15, 2019): 129–48. https://doi.org/https://www.researchgate.net/publication/335960974_Exploring_China%27s_Sharp_Power_Conceptual_Deficiencies_and_Alternatives.

Sutter, Robert. "Barack Obama, Xi Jinping and Donald Trump—Pragmatism Fails as U.S.-China Differences Rise in Prominence." *American Journal of Chinese Studies* 24, no. 2 (2017): 69-85. Accessed July 14, 2021. http://www.jstor.org/stable/44759210.

The Committee on Foreign Investment in the United States (CFIUS). Accessed June 12, 2021. https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

Valeriani, Augusto, and Cristian Vaccari. “Accidental Exposure to Politics on Social Media as Online Participation Equalizer in Germany, Italy, and the United Kingdom.” *New Media & Society* 18, no. 9 (2016): 1857–74. https://doi.org/10.1177/1461444815616223.

Vijay, Darsana, and Alex Gekker. “Playing Politics: How Sabarimala Played Out on TikTok.” *The Dark Social Web: Responsibility, Manipulation, and Participation in Global Digital Spaces* 65: 712–32. Accessed June 14, 2021. https://doi.org/https://doi.org/10.1177/0002764221989769.

Walker, Christopher, and Jessica Ludwig. “Sharp Power Rising Authoritarian Influence.” *Journal Endowment for Democracy*, no. International Forum for Democratic Studies (December 2017).

Walker, Christopher, Shanthi Kalathil, and Jessica Ludwig. “The Cutting Edge of Sharp Power.” *Journal of Democracy*31, no. 1 (January 2020): 124–37. https://doi.org/10.1353/jod.2020.0010.

Wang, Jufang. “From Banning to Regulating TikTok: Addressing Concerns of National Security, Privacy, and Online Harms.” *Platforms, Governance, and Global Society (PGG)*, October 20, 2020, 1–10. https://www.researchgate.net/publication/344584442_From_banning_to_regulating_TikTok_Addressing_concerns_of_national_security_privacy_and_online_harms.

Xu, Vicky Xiuzhong, Fergus Ryan, and Danielle Cave. “Mapping More of China's Tech Giants: AI and Surveillance.” *Australian Strategic Policy Institute*, November 28, 2019, 1–32. https://doi.org/https://www.aspi.org.au/report/mapping-more-chinas-tech-giants.

Yecies, Brian, Michael Keane, Haiqing Yu, Elaine Jing Zhao, Peter Yong Zhong, Susan Leong, and Huan Wu. “The Cultural Power Metric: Toward a Reputational Analysis of China’s Soft Power in the Asia-Pacific.” *Global Media and China* 4, no. 2 (2019): 203–19. https://doi.org/10.1177/2059436419849724.

Zhang, Zongyi. “Infrastructuralization of Tik Tok: Transformation, Power Relationships, and Platformization of Video Entertainment in China.” *Media, Culture & Society* 43, no. 2 (July 21, 2020): 219–36. https://doi.org/10.1177/0163443720939452.