TikTok, It’s Threat to National Security O’Clock

Investigating the Effects of Securitizing Narratives on User Perceptions of Mobile Apps

Jia Rui (Jenny) Tang

Submitted in partial fulfillment of the Prerequisite for Honours in Computer Science under the adviseement of Dr Ada Lerner and Dr Eleanor Birrell

May 2021

©2021 Jia Rui (Jenny) Tang
Abstract

Given the increasing importance of cyberspace in politics, entities such as technology companies and even individual users have become critical pieces in political discourse. Through the securitizing moves made by the United States government regarding Huawei and TikTok, we indeed see the expansion of the national security space to include cyberspace. However, as users of technology have also become referent objects of cyber securitization, we investigate the effects of specific elements in the securitizing narratives surrounding TikTok on user trust in mobile applications. To this end, we ran a user-study on Amazon Mechanical Turk, presenting respondents with an argument regarding allegedly concerning data collection practices of an app, varying the app’s nationality, the tone and language with which the claims were presented, and whether the argument included claims that a government had access to user data. We found that directly presenting users with arguments about concerning data collection practices of an app was always persuasive in significantly decreasing user trust. We further found a strong correlation between an app being Chinese and lower levels of trust. Although users were generally more convinced to reduce their trust in an app when they believed any government had access to their data, users were less trustful of the Chinese government having access than the US government doing so. We also find that those who used an app at least several times a day were less likely to be convinced by any arguments, whether related to securitized entities or not. These results reveal the effects of securitizing narratives surrounding technological actors on the general American populace, and specific suspicions surrounding claims of Chinese government access to American data.
Acknowledgements

Although I may have written over a hundred pages of words, I still cannot find the ones to express how grateful I am to everyone who supported me over the course of this thesis.

I have been so fortunate to have Professor Ada Lerner and Professor Eleanor Birrell as my amazing thesis advisors. I cannot thank the both of you enough for your advice and guidance. I deeply appreciate you letting me pursue my interdisciplinary interests and listening to me get off-topic regarding political science theory and various other topics. I am also so deeply lucky to have been one of your research students and have had you as my mentors—I have learned so much from both of you, and I hope I am not only a better researcher, but also a better person for it.

Thank you to Professor Stacie Goddard, Professor Eni Mustafaraj, and Professor Catherine Delcourt, for agreeing to serve on my thesis committee. Your advice, encouragement, and guidance has been critical and so, so helpful. I also want to thank all the Wellesley professors who generously took the time to help and give advice on this thesis despite being under absolutely no obligation to do so.

To all my friends who have had to listen to my (un)necessary and incessant complaining and stressing throughout the entire thesis process—thank you, and sorry you had to go through that. I promise my personality consists of more than this thesis! To the McAfriends and Millenihilists, your cheer, support, and good humour throughout this thesis, and even far before that, has been invaluable.

To my family, thank you for all of your love and support. I could not have done this without you.

Of course, a thank you to my poor laptop computer, which has steadfastly managed to hold on and continue functioning through these “unprecedented times” even when I myself could not.

There are not enough words to express my gratitude, not in English, not in any language, and not even if I had a hundred pages or a hundred years. So please, to everyone who helped me over this journey, accept my gratitude—much too great to be encapsulated in the words “thank you”—and know that I really, truly mean it.
# Contents

Abstract ................................................................. ii  
Acknowledgements ................................................... iii  

1 Introduction ........................................................ 1  
1.1 Securitization or Privacy Concerns? .......................... 2  
1.2 Research Questions and Design ................................. 4  
1.3 Contributions ..................................................... 8  
1.4 Outline ............................................................. 11  

2 Background ......................................................... 13  
2.1 Securitization ..................................................... 14  
2.1.1 Securitization in Cyber ........................................ 15  
2.1.2 Securitization of China ........................................ 18  
2.2 Online Discourse Surrounding TikTok .......................... 22  
2.2.1 TikTok’s Actual Practices ..................................... 23  
2.3 Fears of Data Collection .......................................... 25  

3 Related Works ..................................................... 27  
3.1 What is Trust? ...................................................... 27  
3.1.1 Baby Don’t Hurt Me (No More) .............................. 28  
3.1.2 Take (a Risk) on Me ........................................... 29  
3.1.3 All About that Context ........................................ 29
5.3.1 Government Access to Data ............................................ 71
5.3.2 Securitization ............................................................... 73
5.4 Assessment of Data Collection ........................................... 75
5.4.1 Lower Trust Due to Recipient of Data ............................... 78
5.5 Effects of Personal Relevance ............................................ 79
5.5.1 Usage of App Moderates Effects of App Nationality .......... 83
5.6 Demographic Effects .......................................................... 85

6 Discussion ............................................................... 87
6.1 Nationality ................................................................. 88
6.1.1 Differences in Initial Trust Between TikTok and Instagram ... 89
6.1.2 Overall Trust Levels ..................................................... 91
6.2 Government Access to Data .............................................. 92
6.3 Securitization ............................................................... 94
6.4 Language ................................................................. 95
6.5 Personal Relevance to App .............................................. 96
6.6 Technical Background ..................................................... 99
6.7 Data Collection ............................................................ 100
6.8 Political Implications ..................................................... 102

7 Limitations and Future Directions ........................................ 105
7.1 Survey Design ............................................................. 105
7.1.1 Attention Check ....................................................... 105
7.1.2 Language Variable ..................................................... 106
7.1.3 Personal Relevance ..................................................... 107
7.2 Data Analysis ............................................................. 108
7.2.1 Likert-type Variables ................................................... 108
7.2.2 Evaluating and Comparing Persuasiveness of Arguments ... 108
Chapter 1

Introduction

In August 2020, former US President Donald Trump declared that the popular social media application TikTok “continues to threaten the national security, foreign policy, and economy of the United States” [83]. This claim came from the “Executive Order on Addressing the Threat Posed by TikTok” (Executive Order 13942), also known colloquially as the “TikTok ban,” which announced that any transaction with ByteDance, the Chinese company that owns TikTok, was to be prohibited in 45 days [83]. On the same day, Executive Order 13943 was signed, detailing the same actions against WeChat, another Chinese-owned mobile application [84]. The issuance of these Executive Orders reveal a trend in the continued securitization of technology, particularly of Chinese technology, in American politics, framing the Chinese companies that own this technology as an existential threat to the United States [12, 3].

Inspired by the TikTok ban and the public discourse surrounding it, this thesis aims to investigate the factors that make arguments relating to supposedly dangerous data collection practices of mobile applications persuasive to the general public, and in particular, whether the elements present in securitizing narratives are effective. By securitization, we specifically mean the framing of TikTok as an existential threat to
the United States (whether to national security or to American values) due to its links to China and the Chinese government. As Americans have similarly high levels of distrust regarding Facebook, another company embroiled in negative media coverage, as of TikTok [20], we wanted to know if the distrust of TikTok and other Chinese companies was necessarily due to the securitizing moves being made to connect TikTok explicitly with China, or whether it was simply due to more general concerns about data collection and sharing [20, 80]. In other words, we explored whether the negative perceptions of TikTok arose from these claims being applied to a Chinese app or whether any mobile application, regardless of nationality, would have fared the same if similar arguments were made about it.

The arguments about the dangers of the securitized entities—such as TikTok and WeChat—leaned on (unsubstantiated) claims that data was being collected by these applications and shared with hostile foreign governments and powers (e.g. with the Chinese Communist Party) [82, 83, 84]. Although users are generally aware of, and suspicious about, their data being collected by technology companies and mobile applications [32, 36], these claims push it into the realm of national security. This framing thus increased the stakes of potential data collection for general users, and could also be used as a justification for otherwise extraordinary government actions taken against what is now framed as an existential threat.

1.1 Securitization or Privacy Concerns?

Although there had already been controversy over TikTok online, mostly around the algorithm and censorship concerns, a turning point in the discourse occurred in the summer of 2020. In a July 7 interview with Fox News, former Secretary of State Mike Pompeo remarked that the Trump administration was “looking at” banning TikTok [8]. He further stated that Americans should use Chinese social
media apps such as TikTok “Only if you want your private information in the hands of the Chinese Communist Party” [8]. This turned the focus onto collection of user data, and also explicitly made prominent the Trump administration’s belief of an alleged link between TikTok and the Chinese government. At around the same time, online discussion around TikTok took a fairly drastic turn. In particular, one Reddit comment in the r/videos subreddit under the post “Not new news, but tbh if you have tiktok, just get rid of it” gained immense amounts of traction online [80]. Originally posted on April 8, 2020, the comment became viral in late June, spreading to other social media platforms such as Twitter and Tumblr, and circulating widely on those as well [57, 75].

From these events, we extract two major securitizing moves being made against TikTok, though both are connected. The first was calling attention to its data collection practices and alleging that this data was being shared with the Chinese Communist Party [83]. This moved the concern beyond mere infringement of user privacy into national security and threat territory, with the threat being not the data collection itself, but rather that it was being shared with the Chinese government, leading to potentially disastrous consequences. The other axis involved the alleged censorship of data deemed sensitive “such as content concerning protests in Hong Kong and China’s treatment of Uyghurs and other Muslim minorities” [83]. This reveals a more general linking of the app to China and the Chinese government, which is an entity that has already been securitized [12, 3]. This securitizing move more broadly underscores the ideological differences between China and the United States, with the threat arising from the fact that the app itself is Chinese, and anything with ties to the Chinese government or supports its actions is presented as antithetical to the American way of life.

The data collection itself seemed innocuous enough (whether from EO 13942 or the Reddit comment) as the data stated to be collected (“including Internet and other
network activity information such as location data and browsing and search histories”) was not widely out of the norm for most social media apps [83], yet the reactions to data collection were widespread alarm. We wonder whether this alarm was because it was explicitly claimed to be sharing data with the Chinese government. In fact, the original viral Reddit comment itself never made any mention of China, but when it became viral months after its original posting, the focus turned to its Chinese ties [80] and thus revealed the link between TikTok and the Chinese government present in the minds of certain users at this time. This led us to suspect that the alarm around TikTok was not due to the data collection itself, but rather that the data collection was by a Chinese company, and believed to be going to the Chinese government. Thus, if the threat perception came from the fact that the data was being shared with not just any government, but specifically the Chinese government, then it would mean that this element of the securitizing move was convincing. Another explanation would be that the alarm simply arose because the app had ties to the Chinese government, which has already been portrayed as an existential threat in US political discourse. Therefore, any explicit linkage of something to the Chinese government would broadly increase distrust. Either would have shown that the persuasiveness and resonance of the arguments came from the securitizing narratives themselves rather than general concerns over user privacy.

1.2 Research Questions and Design

We thus wanted to measure and quantify the effects of Trump’s securitization of technology, and in particular of Chinese technology. We did so by presenting individuals with arguments regarding the data collection behaviour of an app, which variously included or did not include certain elements of interest present in the securitizing narratives surrounding TikTok, namely that TikTok was Chinese, the alarming tone
of argumentation that indicated assumption of malfeasance in TikTok’s data collection practices, and finally, the alleged transfer of user data to a government. This allowed us to test whether it was those particular variables that made the arguments persuasive in convincing someone an app was not trustworthy. We further asked respondents how much data they believed the app collected, as all arguments presented the same facts regarding what data the app collected, and we were interested in whether user interpretations of the same facts would differ depending on framing. We also identified characteristics of the users, such as how frequently they used the app, to understand whether relevance to the issue presented affected effectiveness of arguments.

On one axis regarding elements of securitization, we investigated whether these worries were unique to Chinese apps, and whether users would be less distrustful of the same practices by an American app. Thus, our first independent variable was that of app nationality, using the same arguments for a Chinese app (selected to be TikTok) and an American app (selected to be Instagram, an American social media app with parallels to TikTok). This investigated the broader securitizing move that posited that TikTok was perceived as a threat simply because was it linked to China.

Another element that appeared in the discourse surrounding TikTok, and was particularly evident in the Reddit comment, was the implication that TikTok’s data collection practices were in some sense alarming and out of the norm. The Reddit comment couched its argumentation in relatively more technified language, presenting the user’s conclusions about TikTok’s malfeasance as fact because the commenter was a self-proclaimed “nerd who figures out how apps work for a job” [80]. Thus, due to the relatively more technical way the issue was presented, with ample use of seemingly esoteric technical terms, those with “expertise” were able to frame the discussion, with lay users relying on these experts to relay whether an issue was one of concern due to possible lack of confidence in their own ability to parse the specific technical
Therefore, we wanted to know if this alarmist framing of (relatively common) data collection practices was influential in making the arguments resonate with general users and decreasing trust. We thus decided to vary the language and tone with which the claims were presented to users as our second independent variable, while keeping the information conveyed the same.

As many of the securitizing moves made against Chinese technology companies hinged upon alleged ties to, and the sharing of data with, the Chinese government, we also added in a third independent variable wherein some users encountered an extra argument specifically stating that the government of the respective app may have access to user data. Indeed, as there also exists general American distrust of US government access to data [6], it could be that any government access to user data, regardless of government, reduces trust. Therefore, to understand if it was specifically the securitizing move that was decreasing trust rather than overall wariness of government interference, we compared between the conditions that stated the data was being shared with the US government and ones that stated the data was being shared with the Chinese government.

This thesis thus focused on the effects of these three main variables in influencing users to decrease their trust of certain apps: the nationality of the app, the tone/language of the argument presented to the user, and claims that user data would be shared with a government. This can further reveal how political discourse and securitization arguments in particular could affect public opinion and thus the regulation of apps and technology. Our analysis focused on exploring three main research questions as related to these variables, their influence on public opinion, and the discussions around technology. We were broadly interested in each of our independent variables’ effects, and so we ask:

**RQ1**: What factors are effective in convincing users to be less trustful of an app?
In attempting to disentangle the multitude of securitizing moves that were made against TikTok, we focused specifically on comparisons between TikTok and Instagram to understand whether it was the securitization that made it so worthy of distrust. The key elements present in the securitizing narrative come out most strongly in the nationality variable (the app being owned by a Chinese company) and the interaction of that variable with the government access variable (claims that the data collected by the application is being shared with the Chinese government specifically). If reactions and trust levels were around the same when the same arguments were applied to an American app as a Chinese app, then the fears and distrust surrounding TikTok would not necessarily have been due to the securitization moves being made against TikTok and China, but rather concerns about data collection and use by tech companies overall. However, if there is a difference, then that would imply that securitization arguments are effective in that they manage to reduce trust, or at least amplify concerns. This is specifically explored in RQ2, which aimed to understand if the actions and reactions by the US government and the public surrounding TikTok and Huawei (another Chinese technology company that encountered similar securitizing moves) were specifically due to their status as Chinese companies. Thus, we ask:

**RQ2: Are arguments more persuasive when they claim securitized actors have access to user data?**

Furthermore, as the political discourse around both TikTok or Huawei were similar, it must be noted that while government actions were taken against Huawei (adding it to the Entity List) [85], ultimately the US government was neither able to actually ban TikTok nor force its sale to an American company. Thus, in RQ3, we investigate whether this disparity in the outcomes was due to the broader appeal of TikTok than Huawei. As posited by the elaboration likelihood model, a commonly-used model for understanding persuasion, the amount of personal relevance an issue has to the
individual affects their processing of the persuading argument, and those with more relevance more carefully evaluate the actual claims presented in the argument rather than relying on other cues [62]. In other words, as more Americans use TikTok, the higher personal relevance of the application to American users may have constrained the effects of the securitizing moves, making them less effective. Therefore, our final research question asks:

**RQ3:** Are those with high personal relevance to an application less persuaded by negative arguments towards the app?

### 1.3 Contributions

Though there has been a substantial body of work in both Computer Science and Political Science on the influence of technology—and in particular of social media—on politics and political processes, there has been relatively little work on the other direction of that relationship, investigating the influence of politics on technology and the ways in which people interact with it. Of course, there has been some work on the broader influence of the European Union’s General Data Protection Regulation (GDPR), though much of that has focused on its higher level impact, such as on the length of privacy policies or the ways in which websites have attempted to comply [44, 56, 18]. Most work in this vein have further focused on user behaviour and changes in services that impact users rather than the direct effects of policies on user trust and understandings of the issue. Thus, there is currently little to no work on political decisions, particularly in the realm of national security, as impacts and affects individual users of technology. This thesis addresses this gap in the literature, bringing an interdisciplinary perspective to understanding the relation between policy and technology. With the continued US and Western positioning of certain foreign states, notably China and Russia, as threats in the cyber domain [78, 79, 3], it is
imperative to ask what the effects of this political discourse has on how users perceive technology associated with these nations.

Thus, we take into consideration existing events to ask our questions, and build an understanding of user perceptions of technology that is not divorced from sociopolitical context. Though we explore specific apps (TikTok and Instagram) so as to concretely understand specific real-word happenings and context, we draw upon established political science and computer science frameworks to build more generalizable models. We thus view the main contributions of this work as such: exploring the role of political context and securitizing narratives as a factors in influencing user trust, identifying specific actors that users are concerned about having access to their data, and understanding the relationship between how frequently individuals use an app and their trust in an app.

To this end, we conducted a user study of 829 participants on Amazon Mechanic Turk to explore the persuasiveness of different arguments regarding the data collection practices of mobile apps. All of these participants were US residents. Each participant was presented with one of eight arguments about the data collection practices of a mobile application, with the conditions constructed through combinations of the presence or absence of each of our three independent variables. However, the information regarding what data the app collected remained constant across all conditions. We measured their trust in the app and perception of the app’s data collection both before and after the treatment to understand both overall distributions of trust as well as changes in trust. We define persuasiveness of an argument as a significant decrease in trust for each user within a condition. Thus, an argument was deemed persuasive if a user’s trust in the app went from believing the app was (very or somewhat) trustworthy to neutral, from being neutral to believing the app was (very or somewhat) untrustworthy, or from believing the app was trustworthy to believing it was untrustworthy. We further compared effectiveness across conditions and variables.
by comparing the proportion of users that were persuaded by the various arguments. We also explored pairwise distributions of overall trust levels to understand differences and similarities in general views across conditions.

We found that all eight of our arguments were broadly persuasive, decreasing users’ trust in the mobile application. Of our independent variables, the app which users saw was the only one with differences in initial trust levels, in part because it was the only variable that users were exposed to before measurement of initial trust, as we needed to ask about their trust in a specific app. The initial trust in the apps differed significantly, with much lower proportions of users trusting TikTok even before being presented with an argument regarding the app’s data collection practices. We believe this discrepancy in preformed opinions regarding apps may be because these users were likely already persuaded by the rhetoric surrounding TikTok. However, it is unclear whether this was due to securitization specifically or merely overall negative media coverage. However, we found that the nationality of the app did not matter when controlling for initial trust, meaning that for users who initially trusted the app, persuasiveness of arguments regarding an app were not affected by its nationality.

Claims that a government had access to user data was always more effective in decreasing trust than arguments without such claims, regardless of which government. However, our results also suggest that even though the same amount of data is believed to be shared with either government, users are somewhat less trustful of this data going to the Chinese government rather than the US government. Indeed, as the amount of data users believed the app collected did not vary across most variables, this suggests it was not merely the awareness of data collection alone that was alarming to users. However, across these same variables, trust levels were different. This suggests that trust is not only influenced by the amount of data users thought was collected, but also other factors—particularly the recipient of that data. This further lends
credence to the idea that securitizing moves specifically invoking the threat of the Chinese government having access to users’ data were more effective.

Users with higher relevance to an app (measured by usage frequency of an app), were also in general more likely to find an app trustworthy and less likely to be persuaded by arguments. In particular, those who used the app at least several times a day were similar across apps, regardless of whether they saw TikTok or Instagram, and did not find securitizing arguments more persuasive. Our results also suggest that those who have never used the app are similar in that general arguments about the threatening nature of the app were broadly extremely persuasive, even without including securitizing elements. This shines some light on the disparate outcomes from the securitization of Huawei and TikTok, one of which was relatively unknown in the United States, while the other was much more popular.

1.4 Outline

In Section 2, we give a more comprehensive overview of securitization theory, with a particular focus on how it has been used in the realm of cyber and the relatively unique framings that cyberspace affords. We also explore the ways in which China and specifically the Chinese government have been securitized in US political discourse in recent years. We apply this framework to the case of Huawei as an example of how to evaluate and understand the securitizing moves against Chinese technology companies and then look at some elements of the TikTok ban that fit into this framework.

In Section 3, we give a broad overview of the literature exploring trust, with a specific focus on the factors that influence user trust, and the way users evaluate risk and threat of online interactions and the threat actors. We further tie this into the political science literature on securitization theory in cyberspace.

Section 4 gives a detailed explanation of our methodology and our decisions for the
survey and data analysis. Our results can be found in Section 5, while the limitations of our study and data are discussed in Section 7.

Our discussion section (Section 6), more clearly contextualizes our results through the lens of understanding the effects of securitization arguments being made about and against Chinese technology and companies. It also explores the instances where a securitizing explanation may fall short in explaining the policies and formation public opinion surrounding TikTok.

We conclude in Section 8 with a high-level overview of our study, and some reflections on the implications of our findings and how it may relate to US policy direction as well as the responsibility of technologists and policymakers in this domain.
Chapter 2

Background

Over the course of the Trump administration, we have seen the continued use of protectionist rhetoric and policy by the US government, with a particular target being China and the Chinese government. Former US president Donald Trump consistently identified China as a threat to US interests across many domains, with the Executive Order banning TikTok specifically detailing that “the spread in the United States of mobile applications developed and owned by companies in the People’s Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States” [83]. Such a statement, though incendiary, was not unexpected, but rather a continuation of the securitization of entities related to China [12, 3, 37]. Thus, the rise of negative feeling against TikTok did not begin on August 6, 2020, with the issuance of Executive Order 13942. Rather, existing nationalistic rhetoric surrounding China and Chinese companies laid the groundwork for broad negative feelings by the public, and the justification of otherwise extraordinary actions taken against TikTok in the name of national security [12]. This was possibly compounded by the COVID-19 pandemic, during which we saw a rise in anti-Asian sentiment in the United States, along with rising distrust of the Chinese government and increased instances of anti-Asian hate crimes [65, 72]. Thus, we explore the securitizing nar-
ratives surrounding China as a framework for understanding the persuasiveness and spread of the arguments regarding TikTok.

2.1 Securitization

In political science, securitization occurs “when a securitizing actor uses a rhetoric of existential threat and thereby takes an issue out of what under those conditions is ‘normal politics’ ” [9]. Securitization of an issue allows for the legitimization of emergency measures that otherwise would not have been acceptable [9]. In this case, technology from China (and particularly TikTok and WeChat) were stated to be threats to the American people and US national security, allowing the US government to attempt to ban these entities and the companies behind them. Compounded with the establishment of China and its rise as a global power as existential threats to the United States and the American way of life, the category of what constitutes an existential threat was extended to Chinese companies and apps through claims of their ties to the Chinese government [79, 78].

However, statements from the political elite claiming an issue is an existential threat is not in itself sufficient to securitize the supposed threat. “A discourse that takes the form of presenting something as an existential threat to a referent object does not by itself create securitization—this is a securitizing move, but this issue is securitized only if and when the audience accepts it as such” [9]. Therefore, the securitizing actor also has to convince the American population that TikTok was indeed a threat for the securitization to be considered successful. Nevertheless, as securitizing moves are made in order to increase government latitude in action taken against the securitized entity, it is not necessary for the entire population to be persuaded, but rather just a significant enough portion such that any government action now falls within the realms of legitimacy. Thus, though we do not ultimately measure
whether TikTok was securitized, we explore the effects of key elements present in
the securitization narrative on Americans’ trust of the app. In doing so, we wanted
to evaluate whether arguments including such elements would be broadly accepted
and resonate with the American population, and whether users were more willing to
accept arguments about the lack of trustworthiness of a securitized actor.

2.1.1 Securitization in Cyber

Of particular interest is securitization in the domain of cyber due to certain relatively
unique affordances it offers to securitizing narratives [29]. Despite individuals, rather
than the more traditional nation-state, being the referent object of threat, through
various approaches and framings, entities (whether individuals or collectives) in cy-
erspace have become linked with national security and threats to these objects tied
with threats to the nation [22]. Hansen and Nissenbaum were the first to clearly
articulate some of the mechanisms through which this securitization in cyberspace
occurs [29]. They identify the ways in which cybersecurity concepts such as the net-
work and the individual (the referent objects in cyber securitization) are linked to
national and state security (more traditional referent objects), making securitization
successful, yet also take on a distinct role, in the cyber realm.

One method is through that of hypersecuritization, with “multi-dimensional cyber
disaster scenarios that pack a long list of severe threats into a monumental cascading
sequence” [29] leading to catastrophic outcomes. This is commonly seen through
these hypothesized occurrences being likened to a “cyber Pearl Habor” or a “cyber
9/11.” Although none of these doomsday scenarios have happened, the fear of some
small vulnerability leading to cascading failures and threats gives credence to the
necessity of extraordinary action before it is too late. As risks with physical world
analogues were seen to be more threatening by general users [26], this likely also
contributes to the resonance of terms such as “cyber Pearl Harbor” and “cyber 9/11”
in constructing an unimaginably horrible existential threat and justifying extreme measures to protect against such catastrophes.

Another grammar of cyber security occurs through what Hansen and Nissenbaum term *everyday security practices*, involving “the securitizations of everyday digital life with its dangers of credit card fraud, identity theft, and email scamming” [29]. Though these events involve harm to individuals, they are construed as threats to the entire network and hence, society. Thus, each individual becomes responsible and tied to the collective fight against insecurity in cyberspace. This is linked to hypersecuritization as threat to any one citizen could cause cascading consequences. Therefore, though the referent object may be an individual, the threat becomes to an entire collective such as the nation and thus worthy of securitization.

The third avenue is that of technification. Due to the relative expertise required to master the field of computer security, deference of the topic is given to technical experts. This thus “constructs the technical as a domain requiring an expertise that the public (and most politicians) do not have and this in turn allows “experts” to become securitizing actors” [29]. Through this technification of cyber discourse, the securitizing rhetoric is portrayed as objective rather than political, making it more difficult for general users to challenge the securitizing move. Indeed, though traditional securitization theory emphasizes securitizing moves by political elites through official statements, the legitimization of the threat can also occur through other actors, and particularly technical experts in cyber [22]. This allows for the threat to be broadly unchallenged due to users lack of confidence in their ability to parse what may seem to be a complicated technical issue, and leaving it to “experts” to frame and direct the conversation.

“Cyber securitizations are particularly powerful precisely because they involve a double move out of the political realm: from the politicized to the securitized, and from the political to the technified” [29]. Thus, securitization of cyber threats have
become significant in two ways, both as an exceptional threat to the national interest, and exceptional due to the technical expertise necessary to coherently evaluate the threat [41]. However, scholars have noted that there have been increasing attempts to counter the narrative of hypersecuritization of cybersecurity and cyberwar in the past decade, with certain threat scenarios being now seen as less plausible [41]. Nevertheless, cyber securitizations have tended to remain relatively technified, and individual everyday security in cyberspace has continued to be linked to national security in cyberspace.

Within the American context, we have further seen a widening of what referent objects can be considered threatened and thus important to the nation’s security and existence. Indeed, the 2017 US National Security Strategy emphasizes the importance of protecting US data in the interests of national security [78]. It further points out that “China gathers and exploits data on an unrivaled scale” [78]. Thus, with the addition of data (including that of US citizens) as a critical feature to US security, such a move further allows for the possibility of securitizing any entity (such as TikTok) that is seen to be collecting any American data, and not just data in critical sectors such as military or government.

Cyberspace has also been shown to be an area of focus for general Americans’ suspicions of China. Indeed, a Pew Research Center study from March 2021 revealed that cyberattacks from China was the top problem for many Americans, with 91% believing it to be a problem and almost two-thirds of all Americans (65%) considering it to be a “very serious” problem [73]. This suggests the existence of suspicion regarding Chinese cyber activities specifically, and may thus be indicative of relatively successful securitization of China as a threat in the digital realm.
2.1.2 Securitization of China

Moves to securitize China are plain to see in recent US policy, arising in part due to fears of rising Chinese dominance and a possible shift away from a global order dominated by the American leviathan [3]. However, the existential threat not only comes from China’s growing economic, military, and technological power in competition with the United States, but also because its ideologies are viewed antithetical and threatening to the American way of life. Specifically, US political discourse claims “China’s communist credentials serve to place it and its companies in opposition to US interests” [12]. Therefore, this rhetoric broadens the scope of perceived Chinese threat beyond specific domains of strategic importance such as commerce or warfare, and now the threat arises simply due to the fact of the securitized entity (e.g. a company) being Chinese.

Campion outlines numerous similarities in the successful securitization of Chinese companies China National Offshore Oil Corporation (CNOOC) and Huawei [12]. Suspicion was cast upon the companies due to their Chinese ownership, drawing explicit links between the companies and an allegedly threatening actor. Due to the success of these companies in their fields, they were viewed as examples of Chinese success abroad and the spread of Chinese influence. Both companies furthermore operated in areas considered to be part of US critical infrastructure (energy and telecommunications), allowing for more extreme government measures. There are thus many similarities in the steps taken against these Chinese companies and those applied to TikTok, though with varying degrees of success and some notable differences. We explore in more detail the securitization of Huawei, and the processes and narratives that led to it being added to the Entity List in 2019.
Securitization of Huawei

One example of the successful securitization of a Chinese company would be that of Huawei. Similar to TikTok, concerns about Huawei centered around its alleged ties to the Chinese government. From a February 2018 Senate Intelligence Committee hearing, it was stated that Chinese telecom companies such as ZTE and Huawei were understood to have “extraordinary ties to the Chinese government” [70]. As these concerns revolved around “the close relationship between the Chinese government and Chinese technology firms” [70], such rhetoric tied a new existential threat (Huawei) to a well-established one (China), making the securitizing move easier. There were further accusations that it had close ties with the People’s Liberation Army (PLA), and the fact that Huawei’s founder, Ren Zhengfei, is an ex-PLA member has further allowed for increased suspicion of Huawei and that it was under Chinese government control [37]. The securitization of Huawei arose also in part due to the dominance of Chinese companies in the area of 5G [12]. Due to the relative lack of American competitors, the American intelligence community was worried about the “risks of allowing any company or entity that is beholden to foreign governments that don’t share our values” to “exert pressure or control over our telecommunications infrastructure” [70].

The possible capability of such an entity to exfiltrate data was also raised as a possible concern, though unlike for TikTok, it was not the main move [70]. Rather, the securitization of Huawei was justified insofar as it was believed to be beholden to the Chinese government. Nevertheless, despite theories about Huawei’s intentions, and assumptions that exported technology from China would have backdoors, there has yet to be a backdoor found in Huawei’s products [76].

This culminated in an Executive Order issued on May 19, 2019, titled “Securing the Information and Communications Technology and Services Supply Chain” which stated that the ability for foreign adversaries to “create and exploit vulnerabilities in
information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States” [82]. This falls neatly into the hypersecuritization grammar used in the securitization of cyberspace, and firmly shows Trump’s willingness and ability to securitize foreign technology. Furthermore, the Executive Order stated that the “threat exists both in the case of individual acquisitions or uses of such technology or services, and when acquisitions or uses of such technologies are considered as a class” [82]. This reveals the use of everyday security practices being used to securitize technology, and bringing the individual as relevant to broader security concerns in cyberspace.

Although Executive Order 13873 did not explicitly name Huawei nor China, it implicated them, as cyber threats have often been tied to either Russia or China in American political framing [79]. Furthermore, less than a week after the issuance of the Executive Order, the Department of Commerce added Huawei and its subsidiaries to the Entity List, as it states there existed reasonable evidence that “Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States” [85]. This then effectively prohibited Huawei from engaging in transactions with US companies without US government approval.

While other nations, notably the UK, have debated the use of Chinese companies within their 5G networks, the US distinguishes itself by framing the company Huawei itself as the existential threat rather than its potential role in critical infrastructure [12]. In this securitization of Huawei, there are a few pieces of note. First, it was stated to have ties to an already securitized actor (the Chinese government), making any of its actions therefore possibly dangerous. Though possible access to sensitive American data was raised as a concern, the main threat framing around Huawei appeared to be that it could exert a certain amount of control over telecommunications infrastructure due to its prominence in the 5G sector. It was only with TikTok that collection of
data became the main threat around which the securitizing move was made.

However, Huawei differs from TikTok in a few key areas. The case against TikTok appeared amid rising anti-Asian, and specifically anti-China sentiment, in part due to the COVID-19 pandemic. In April 2020, 66% of Americans held unfavourable views toward China, which rose to 73% in July 2020, which was 26% points higher than in 2018 [19, 72]. Furthermore, around 90% of Americans saw China’s power and influence as a threat, and 62% believed that it was a major threat [19]. Lastly, compared to 2012, where 15% of Americans viewed China as an enemy, in 2020 26% of Americans did so, and this number rose further to 36% in 2021 [72]. These statistics all serve to show increased suspicion and distrust of China over the course of the COVID-19 pandemic. Though this distrust was not caused solely by the securitization of China throughout the Trump administration, it nevertheless shows that at the time these securitizing moves were being made against TikTok, the US population held broadly negative views, and perhaps were more willing to accept negative arguments against companies, entities, and even people perceived to have ties with China. Yet despite this broader distrust of China during the proposed TikTok ban, it was ultimately unsuccessful, unlike with Huawei. This may be in part due to Huawei’s lack of relevance to general American consumers. Indeed, “the first that many Americans heard of Huawei was in reports linking it to threats to US national security” [12], whereas TikTok had been popular and well-established as a social media platform before summer 2020. Thus, we look at some of the arguments made regarding TikTok, keeping both the context of the pandemic as well as the app’s broader popularity among Americans in mind.
2.2 Online Discourse Surrounding TikTok

In the case of TikTok, the linkage of everyday security practices and individual dangers to collective national security concerns, as well as the technification of arguments regarding data collection, appear the most prevalent. One particular instance that shines light onto the phenomenon of rising distrust in TikTok can be traced to a Reddit comment posted in April by Redditor u/bangorlol [80]. It stated, using very alarming language, that TikTok “is a data collection service that is thinly-veiled as a social network” [80]. However, it did not garner much attention online until a few months after its original posting. It was screenshotted and posted to Twitter by Twitter user @d1rtrydan on June 27, 2020 [57], and currently has over 60,000 retweets, 10,000 quote retweets, and 100,000 likes. This tweet was then further posted to another social networking site, Tumblr, on June 28 by Tumblr user invertedporcupine, to which the original Reddit comment and text was added by squareallworthy, and also garnered over 45,000 notes [75]. The original Reddit comment currently has over 28,000 karma and over 140 (Reddit) awards. The full text of the comment can be found in Appendix A.2.

From these numbers, it is evident that something in the argument resonated with broad swathes of people across social media platforms, but only when the debate and media storm around TikTok and its ties to China became prominent. Much of the fears of the Reddit post focused on the allegedly concerning data collection practices of TikTok, but made no mention of China. Thus, there were two broad fears in online alarm regarding TikTok. The first was that TikTok collected too much data, and this was present in the Reddit comment. These concerns tie into the way Trump has made securitizing moves in cyber by moving American data into the realm of of national security and of national interest [12, 78]. The second fear was that this user data was being shared with the Chinese government. This second concern was thus not over just any access to data, but specifically Chinese government access, and was what
drove attention to the claims in the Reddit comment, despite it not being originally part of the discussion. This thus suggests it is not the data collection alone that made the claims of the comment persuasive to people, but the implications of certain recipients accessing that data (allegedly the Chinese Communist Party).

We further see the effects of technification in increasing the saliency of the Reddit comment, as the poster claimed “I’m a nerd who figures out how apps work for a job” and had “reverse-engineered the app,” using technical terminology to make their case [80]. Indeed, lay users, despite concerns for their online security and privacy, are often unable to clearly articulate the technical threats, and thus may rely more on the framing of expert users in assessing risk [30]. Thus, these cues appeared to give more credibility to the claims made, as many individuals would not necessarily have felt confident parsing the exact technical details, instead deferring to the expertise of “experts,” even self-proclaimed ones. However, not all experts agreed with this analysis of TikTok’s alleged malfeasance.

2.2.1 TikTok’s Actual Practices

Much of the evidence pointed to regarding TikTok’s malicious behaviour and concerning data collection practices seem to originate from either the Reddit comment [80], a blog post by security company Zimperium [71], or from a security analysis whitepaper from a firm called Penetrum LLC [61]. However, there was also evidence that TikTok’s practices were not out of the ordinary, though none of these gained nearly as much traction as did the ones covering TikTok negatively [43, 21, 50, 1].

Although Zimperium, a fairly established security company, stated that “the Android version has high privacy and security risks and iOS has high privacy and medium security risks. iOS rates 98/100 for privacy and 64/100 for security. Android is 79/100 for privacy and 82/100 for security” with higher numbers being more concerning, they did not make explicit claims about any ties to the Chinese government [71]. Further-
more, they did not position the risks of TikTok as unique in the app ecosystem.

On the other hand, the Penetrum paper attempted to explicitly link TikTok with threatening Chinese entities and malicious data collection [61]. However, this whitepaper did not provide any concrete proof of such ties, but implied that it was alarming that TikTok appears to store some data on cloud services provided by Alibaba, another Chinese company. Indeed, Penetrum is the only “expert” technical source that specifically attempted to tie TikTok data collection to China. Furthermore, a large portion of the whitepaper’s claims regarding suspicious and unnecessary data collection comes from the fact that TikTok uses trackers from AppsFlyer, yet AppsFlyer is an American company, and partners with myriad other companies, such as Facebook, Google, and Adobe [5]. Thus, the issues found by Penetrum were not limited to TikTok. Lastly, the company itself does not seem to be well-established, with very little information surrounding it apart from its brief prominence as evidence for the malicious practices of TikTok. Nevertheless, despite the overall lack of credibility present in the paper, it was picked up and widely circulated in the Reddit community as “evidence” of TikTok’s evil deeds, possibly in part due to the relatively technical language it used. This shows the strength of technification in cyber securitization in that any actor with enough technical credibility has the ability to frame the conversation and present misleading information without being deeply questioned due to the perceived hard-to-understand technical nature of the issue.

Despite the fearmongering surrounding TikTok, scholars and other experts have consistently found no evidence that TikTok’s data collection and security practices are worse than that of other mobile applications [43, 21, 50, 1]. The general consensus appeared to be that “TikTok’s data collection isn’t great, but it’s not unusual in the app space,” with most other applications collecting the same type of data [50, 1].

To date, the most holistic review of TikTok was conducted by the University of Toronto’s Citizen Lab. It explored both TikTok and Douyin (the Chinese counterpart
to Douyin specific to East and Southeast Asia), publishing their findings in March 2021 [43]. In fact, the Citizen Lab report noted that TikTok’s data collection practices “are not exceptional when compared to industry norms” and the app does “not appear to exhibit overtly malicious behavior” [43]. Neither app collected “contact lists, recording and sending photos, audio, videos or geolocation coordinates without user permission” [43], which refuted the claims made by Penetrum and the Reddit post that TikTok was collecting GPS location data [80, 61]. The report does note that Douyin exhibited certain concerning behaviours, such as server-side search censorship, but the version of the app available globally, TikTok, which was the version being securitized, did not.

Therefore, in spite of claims regarding the nefariousness of TikTok, there has continued to be little evidence that TikTok (the global version of the app at least) does anything out of the ordinary. Yet these concerns continued to be pronounced, so perhaps it was not necessarily the fact that it was TikTok collecting the data that was concerning, but rather any data collection.

2.3 Fears of Data Collection

Even within the reactions to the viral Reddit comment, some users have pointed out that such data collection is common in the mobile app ecosystem, and that many other apps share similar behaviour [86, 1, 50]. However, simply because this type of data collection was not unusual did not necessarily mean that these users trusted TikTok more. Some stated that “While in theory this could be used for tracking people (and I don’t necessarily doubt China’s government is abusing the data provided by apps run out of China), almost all of the data mentioned above is more commonly used to quickly identify and respond to technical issues within the app” [86]. Still others were quick to point out the hypocrisy in the concerns over TikTok’s data collection...
practices simply because it is a Chinese company, “But lately it’s just bc it’s a Chinese owned app, which feels, frankly, racist bc US companies haven’t proved to be more ethical (cough...Facebook)” [50].

Indeed, it would appear that Americans generally distrust companies associated with excessive data collection. Indeed, 42.6% of Americans were found to distrust Facebook, compared with the barely higher 43% that distrusted TikTok [20]. However, a higher percentage of Americans found Facebook (37.8%) trustworthy than felt the same for TikTok (28.1%) [20]. As Facebook has also caught a lot of negative media attention for the Cambridge Analytica scandal and the Federal Trade Commission’s $5 billion penalty in 2019 for Facebook’s violations of user privacy [24], distrust of these companies may have largely been due to repeated exposure to negative media regarding these entities. Interestingly, Americans were split about Huawei, with 30.4% trusting and 30.4% distrusting it. Put into context, more Americans felt Twitter was untrustworthy (31.8%) than did for Huawei, a company that was securitized. This suggests that recency bias may also at play, with higher levels of distrust in companies that were more prominent and received more negative media coverage. The same study further found that 62% of those surveyed believed that social media companies and search engines needed more regulation [20], demonstrating that a majority of Americans were concerned about the collection of their data, regardless of source. Therefore, it is possible that it was not necessarily the fact that TikTok was Chinese that was the main driving factor of distrust, but rather suspicion of any type of data collection, which we investigate further in our study.
Chapter 3

Related Works

In this section, we explore the multi-disciplinary literature surrounding trust and the factors that influence trust, particularly as related to privacy and data collection. In the legal and political science fields, privacy is generally seen as something that must be balanced against other important values, such as freedom and national security, while computer science tends to focus on user perceptions of their control over personal data and user consent regarding the use of said data [74, 47]. Therefore, we synthesize the views between disciplines in our work by focusing on the securitizing narratives made regarding data collection and data sharing, which tie together the framing of privacy as related to national security while also keeping user concern in mind. We also look at literature regarding argumentation and persuasion, with a focus on connecting these understandings to the literature about cyber securitization.

3.1 What is Trust?

There is a large body of work across multiple disciplines on what constitutes trust, with varying ties to security and privacy [69, 89]. Indeed, due to trust’s importance across many various disciplines, being “at once related to dispositions, decisions, behaviors, social networks, and institutions” [69], there have been widely diverging
quantifiers, understandings, and definitions of the concept. We give here a brief overview of the myriad ways in which trust has been understood in the literature, breaking down trust into three main component parts, while recognizing that many definitions conceptualize it as composed of some combination of these components, though with varying emphasis on each.

3.1.1 Baby Don’t Hurt Me (No More)

One line of work focuses on trust as based on the interaction and relation between the actor that is trusting (the trustor) and the actor that is the object of that trust (the trustee), based on actual risks, consequences, and behaviours. This understanding of trust involves the willingness the trustor, to rely on and accept vulnerability to the actor being trusted [69, 67]. A commonly cited definition proposed by Rousseau et al. in this vein states that, “Trust is a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behaviors of another” [69]. Similarly, Riegelsberger et al. conceive of “trust as an attitude of positive expectation that one’s vulnerabilities will not be exploited” [67]. Thus, trustors would only make themselves vulnerable if they believed the trustee is trustworthy [67]. Hoffman et al. further defined trust as “the expectation that a service will be provided or a commitment will be fulfilled” [27], thus moving somewhat away from threat and risk itself, and focusing rather on positive exchanges. More specific to online contexts, trust reflects the belief users have that the company or other trusted party will protect their information, where the possible vulnerability often comes from the unauthorized use of or misuse of data given to the trustee [47]. More recent work has focused on the actual rather than the perceived behaviour of the trusted agent as a basis for trust [35, 42]. For example, Kang et al. used the similarity between expected behaviour and actual behaviour of an application to evaluate trust [35]. This line of work often ties into explorations of trust (and privacy) that investigate
its impact on user behaviour. For our research, the perceived trustworthiness of an app is thus important in understanding whether users are less trusting, and thus less willing to accept vulnerability when interacting with securitized entities.

3.1.2 Take (a Risk) on Me

Related to the acceptance of vulnerability as an aspect of trust, Rousseau et al. identified the presence of risk as a necessary precondition for trust [69]. With perfect knowledge of the outcomes of an interaction, there would be no need to trust an agent. Therefore, “risk creates an opportunity for trust, which leads to risk taking” [69]. This is further backed up by Malhotra et al., who state that “when potential risks are present, trust plays an important role in determining one’s (trusting/risk taking) behaviour” [47]. Therefore, a closely related line of work investigates trust as related to user perceptions of risk, and includes a deeper focus on the predisposition of the user, focusing on trust as varying from individual to individual [89, 38, 47]. This existence of risk also plays into our measurement and evaluation of user trust in that we were curious whether the same amount of data collection would seem riskier (and therefore less trustworthy) if it was said to go to a Chinese company rather than an American one, or specifically to the Chinese government rather than the US government.

3.1.3 All About that Context

Many scholars have also recognized the need to identify the contextual influences, such as social and environmental factors, that play into the building and evaluation of trust [55, 10, 67, 51]. For example, Camp gives one definition of trust “as consisting of privacy, reliability and security” while also stating that it required an “understanding of how social agents (individuals and institutions) participate in and contribute to trust” [10]. In other words, trust may differ by situation, context, and from indi-
vidual to individual. Furthermore, the beliefs regarding the other’s intentions as well as social norms can regulate and constrain the ways in which the parties are likely to behave [69, 47]. The specific context and situation under which an assessment of trust or privacy occurs is also believed to influence the outcome [38]. When thinking about the connecting between trusting beliefs and data collection, this conceptualization necessitates the recognition that social and organizational forces also determine the extent of control one has over the security of their data, and that individual perceptions vary regarding privacy, therefore resulting in different trust perceptions for the same actor. For example, the predictors of user trust for financial services sites and for travel sites differ due to the different contexts in which user data was being collected [7].

To the best of our knowledge, we are the first to look at sociopolitical context, and specifically securitizing narratives, in influencing trust perceptions of technology. Therefore, under this conceptualization of trust, the increased wariness of Big Tech, concerns over control of personal data, as well as rising anti-Asian sentiment from the COVID-pandemic and continued positioning of China as a threat on the global stage [45, 3, 72, 19], all played a role in user assessments of their trust in a mobile app beyond the mere securitizing moves.

3.2 Factors that Influence Trust

As can be seen from these deeply interconnected lines of work in evaluating and defining trust, there are a myriad of factors that play into a individual’s perception of an actor’s trustworthiness. Thus, there exists also a significant amount of literature that investigates what influences user trust, whether it be perceived trust or trusting behaviour. Here, we focus on work that explores user trust and behaviour regarding interactions online or with mobile apps. Most prior work focuses on measuring the
effects of peripheral cues to users (such as website design, manipulation of perceived company reputation etc), and thus this work is unique in presenting users with specific arguments intended to directly impact trust levels. We believe this type of study is necessary due to the politicization of and securitizing narratives surrounding (Chinese) technology, and the media and online discourse regarding these entities, where populations do in fact encounter these types of direct arguments.

3.2.1 Reputation

Reputation has been frequently shown to play an important role in shaping user trust and behaviour, as brands, companies, and apps with better reputations or that are more well-known enjoy higher levels of trust [36, 7, 13, 60]. Reputation, according to Rousseau et al., is in part based on a third-party’s ability or willingness to corroborate the trustworthiness of the trusted party [69]. The trustor’s evaluations of the trusted party, particularly if it is a company, is influenced by their impressions of the company as a whole [52]. In fact, “an individual tends to easily accept the generally held view regarding the reputation of a company and to use it to form an opinion regarding trust in that company” [40], also revealing the social influence on trust, due to the social construction of reputation. When looking at initial interactions between a trustor and trustee, contextual properties such as reputation were most influential in influencing trust, with intrinsic properties becoming more important over time as interactions continue [67].

Indeed, in many contexts, reputation may in fact be the most important cue in determining trust. Koufaris and Hampton-Sousa found that perceived company reputation was the most important factor in an individual’s initial trust of a website [40]. User ratings have also been found to be the most influential driver in consumer decisions to install apps, while brand familiarity was another cue that users relied upon when installing apps [13, 60]. A company or brand’s reputation also appeared
to be more influential than its stated policies (such as privacy policies) in influencing user trust [52].

Most studies that investigated reputation tend to use popularity or how well-known a company is as a proxy for varying reputation [48, 52]. McKnight et al. tested the effects of the reputation of a fictitious legal advice site by varying how popular and highly ranked it was said to be, finding it to a strong positive predictor of trust behaviour [48]. This suggests that information about an actor from others deeply influences trust, and “even second-hand notions regarding the vendor powerfully affect willingness to be vulnerable to the vendor” [48] as the site was in fact not that of an actual legal company. The same was true for an experiment regarding an online music retailer website, which was either that of a known brand or the exact same site with only the name varied to a fictitious one [52].

Therefore, securitizing narratives about an actor may affect trust by reducing the reputation of that entity (in our case, TikTok) through arguments to its lack of trustworthiness due to possible connections with the Chinese government. However, it appears that in much of the computer science literature, reputation has mostly been measure by popularity (how “well-known” a name or brand is), which does not always necessarily cover all aspects that play into the formation of the reputation of the trusted party.

3.2.2 Social Circles and Other Sources

Similar to work on reputation as a determinant of trust, some scholars have evaluated the other social drivers of trust and behaviour which are not as directly related to the trustee (as reputation is). In online shopping scenarios that were information intensive and involved things that were more complex to purchase, such as automobiles, computers, and travel products, advice was an influential driver of trust [7]. Users also accepted security advice from diverse sources as workplaces, domain profession-
als, family and friends, as well as media, including TV shows and movies showing negative events [64]. When deciding whether to accept digital security advice, the trustworthiness of the advice source was the main metric, particularly when users felt unable to evaluate the advice content [64]. Conversations about security and observations of security-preserving behaviour also influenced security awareness and behaviour [15]. Furthermore, past experiences, whether of the individual themselves, stories from friends and family, or media coverage, can influence a user’s risk perception and behaviour [2]. Yet although both people and media can influence perceptions and intended behaviour, Mendel and Toch found that people were more influential than organizations (such as news media, non-profits, or the government) in promoting intended behaviour around protecting online privacy [49].

This body of work regarding media as a source of information suggests that broadly speaking, news coverage of a security issue or technology company influences not only reputation of the company but also user trust. The role of domain experts in disseminating information and advice is also intriguing, particularly as relates to the technification of securitized issues in the cyber domain [29]. This suggests that not only are experts are able to frame and direct discussion, but also that it is successful because lay users would generally find this source credible and use the information propagated by these experts in forming their own views. Furthermore, although such work identifies stories (from media or other people), conversations, and discussions regarding technology as factors that may impact trust and risk perception, they do not fully quantify the effects of these discussions, which we attempt to do in this study.

3.2.3 Design

Another cue that plays into user evaluation of trust is the design of the website or interface of the trusted actor, such as its functional and aesthetic quality, [58, 48].
In fact, website quality has been found to have a significant impact on trust, with McKnight et al. finding it to be the strongest predictor of trusting beliefs in a website [48]. However, some of the influence of design may vary from individual to individual [54]. Nevertheless, generally speaking, amateurish designs decreased credibility of a website, which was defined as “an assessment of both trustworthiness and expertise” [25]. In other words, there is often likely to be lower trust if the trustee looks or feels “sketchy” as indicated through visual cues to the trustor.

### 3.2.4 Individual Predispositions

Design thus ties into differences between individuals in evaluating trust, due to differences in individual predispositions. However, the internal predisposition of a user still has an effect of their privacy perception and thus trust. Murayama et al. developed a model they termed “Anshin” which encapsulated the emotional part of trust, wherein they identified six factors that contributed to a sense of security [54]. Three of these factors, namely experience, preference (for the user interface), and knowledge, were based on the individual’s own preferences and background [54], suggesting that individual factors play a significant role in the formation of trust. Yan et al. further theorized that the degree of willingness an individual would have to interact with a system also factors into trust [90]. Indeed, most of the literature agrees that trusting and risk beliefs are influenced at least somewhat by personal traits [47]. Depending on an individual’s own dispositional factors, behaviour and privacy assessment may differ, and behaviour regarding privacy and security varies because different individuals weigh the risks and benefits differently [38, 23]. Yet the predisposition of individuals may also not be extremely effective, as individual customer trust propensity was not found to have an effect on initial trust of a website [40]. Nevertheless, this may also be due to the fact that initial trust beliefs may change over time over repeated interactions with the trusted party [40]. Therefore, when evaluating individual pre-
dispositions as a factor in influencing trust, it may be prudent to also consider what factors into these predispositions, including the context in which trust and behaviours are measured.

### 3.2.5 Data: Collection and Control

A significant portion of the work on trust in computer science revolves around its connection with privacy, which is often deeply related to a user’s concern over the collection of their personal data and their control over the use of that data [47, 46]. Indeed, on the Internet Users’ Information Privacy Concerns (IUIPC) scale, one main axis measures the user’s concern over the collection of their data relative to the benefits foreseen in providing that information [47]. Another axis, awareness, involved the user’s concern over what the actor to which data is given will do with that data [47]. These two broad concerns allow us to understand these various factors that feed into concerns over data collection and finally into trust. Furthermore, connected with these concerns regarding data collection and control is the trustor’s perception of the actor which is collecting or receiving the data, which also influences perceived trust and privacy [46].

Before any actor is able to potentially maliciously use data or use it in a way that is undesirable to the contributor of that data, the information first has to be collected. Most online shopping consumers were concerned about the secondary use of the data they provide, and 63% of those who do not provide personal information online stated that it was due to lack of trust in those collecting the data [32]. Higher risk furthermore is often associated with the release of more sensitive information [47]. However, the perception of the sensitivity of the data being shared was directly linked to the trusting beliefs, risk beliefs, and the behavioural intent of the user [74]. Therefore, even in the collection of data, depending on what data is being collected, the actor collecting the data, and the individual whose data is being collected, risk
evaluations and thus trust may vary [55].

Supposing that data is successfully collected, especially in the current age wherein most users feel relatively little ability to prevent data collection in daily life [6], the user’s perceived control over this surrendered data becomes important in their trust [47]. A seminal work by Hoffman et al. theorized that the lack of trust arises from consumers feeling little control over their personal information after it is provided to Web merchants [32]. Camp also notes that privacy measures often define it as an individual’s willingness to share information, which assumes that this willingness is evaluated based on the “risk of secondary use of information” [10]. Indeed, privacy risk is highly identified with a loss of control of personal data [74]. Privacy interacts with trust in that privacy was an important determinant of trust in situations where information risk was high, such as travel sites, which require personal information [7]. Therefore, the context of data use becomes important when understanding how privacy and data collection are related to trust. Joinson et al. distinguished between dispositional privacy concerns (i.e. predisposition of a user) and situational factors when predicting user disclosure of information, with results suggesting that they have independent effects on behaviour [34]. They further found that high trust could compensate for perceived lack of privacy in predicting individuals’ privacy behaviour [34].

In sum, it would appear that both the collection and the use of data is a main concern for users, and both these concerns tie into the construct of privacy, broadly speaking, which further influences trust. In the context of our work, the data said to be collected remain constant between conditions. However, depending on the user, the actor collecting the data, and the recipient of that data, the risk and threat perceived in these actions may vary, and this difference can reveal the influence of securitizing rhetoric on trust.
3.3 Risk

Trust and risk are deeply connected, in that higher trust often corresponds with lower risk perception [47]. Furthermore, the threats and risks believed to be incurred also affect trust and behaviour. In fact, certain actors are linked to higher perceptions of risk for users. Unsurprisingly, companies were the most frequently identified threat to online privacy, followed by third parties [36]. Furthermore, around half of all participants surveyed by Kang et al. also mentioned the government as a possible threat [36]. Connected to the importance of control over data to user perceptions of privacy, perceived risk was higher when users felt less control, greater catastrophic potential, and more severity of the hazard [87]. Similarly, Smith et al. found that “calculation of risk involves an assessment of the likelihood of negative consequences as well as the perceived severity of those consequences” [74].

Exposure through media to certain risks also increases user awareness of these risks, with examples being cyberbullying and identity theft [87]. This implies that frequent exposure through media or other experiences to certain risks increase the likelihood of individuals being aware of these hazards, and that the media is a method of transferring knowledge of not only security advice, but also of threat. Perceived risk not only influences trust, but also intentions and behaviour of users, with consumers less likely to conduct transactions with an Internet vendor when risks are believed to be high [48].

Thus, the literature suggests that users also evaluate the risks and associated consequences when assessing their trust in an actor. Trust also influences the willingness of a trustor to bear these risks, depending on the consequences. The importance of assessment of severe consequences is interesting as it relates to hypersecuritization and doomsday scenarios in cyber securitization. When such framing is used, even without needing to clearly articulate the threat and its consequences, the securitizing actor is able to greatly increase the perceived severity of the threat. In addition,
the mere media attention and securitization of TikTok may have also drawn user attention to a previously unarticulated threat, and thus presented another avenue of lowering trust.

3.4 Understanding Persuasion: The Elaboration Likelihood Model

As our study focused on whether the securitizing moves made against TikTok were persuasive, we drew inspiration from the widely-used elaboration likelihood model (ELM) in understanding what makes arguments persuasive to individuals [62]. It is comprehensive, even when used to understand multi-faceted concepts such as trust, in that it takes into account both the characteristics of the recipient of the argument as well as the context of the presented argumentation.

The elaboration likelihood model posits two main ways in which an individual’s attitude may change towards an issue, either through the central route or the peripheral route depending on characteristics of the individual, such as their motivation and ability to evaluate the argument [62]. The term elaboration in this model thus refers to the “extent to which a person thinks about the issue-relevant arguments contained in a message” [62]. When attitude change results from the central route, the individual considers and evaluates the arguments presented, leading to more enduring attitudinal and behavioural changes. On the other hand, persuasion through the peripheral route occurs when the motivation and ability to consider the arguments are low, and thus attitude change occurs due to other peripheral cues in the context, such as the source of the argument, rather than the arguments themselves.

The expertise and relevance an individual has to the issue at hand also affects the likelihood of elaboration. As personal relevance, expertise, and involvement increase, individuals are more likely to consider and process the arguments, in part due to
their ability to actually process the information. Those with lower personal relevance thus are more likely to rely on peripheral cues, such as the message source (for example, whether or not the argument originates from an expert source), the number of arguments, or even the presence of pleasant music.

We briefly give an overview of some work done in the computer science domain using ELM to understand user perceptions and behaviour.

Cheung et al. used it to evaluate the way consumers judged the credibility of online reviews, find that argument quality, a central cue, was the primary factor affecting review credibility, though participants also relied on peripheral cues such as source credibility, review consistency, and review sidedness when evaluating online consumer reviews [14]. As expected from ELM, individuals who were more involved and knowledgeable relied more on central cues such as argument quality. Interestingly, those who were less involved did not necessarily rely more on peripheral cues.

Gu et al. explored the contextual cues (perceived permission sensitivity, permission justification and perceived app popularity) on the privacy concerns of Android users and their behaviour as measured through download intention of applications [28]. In general, perceived privacy sensitivity increased privacy concerns, while the justification of needing these permissions and perceived app popularity decreased concerns. Perceived app popularity, as measured through ranking and number of downloads, also had a positive effect on download intention. They further found that personal relevance, explored through users’ past experiences, played a role in the formation of privacy concerns, with permission justification making users less concerned about their privacy only for those with less mobile privacy victim experience. This reveals that populations with differing personal relevance are affected differently in technological contexts.

Most of the work in the computer science domain on influences in privacy and trust appear to be based on understanding peripheral cues (such as design and reputation)
rather than using explicit arguments to achieve an increase or decrease in trust as we do in our study. Given the general context of user interactions and behaviours online, this is understandable. However, we do not use ELM entirely to evaluate argument persuasiveness because unlike online reviews, most people would likely not be actively seeking out information about TikTok or Instagram, but rather simply encounter them through news media or social media. Thus, though we draw from the theories of ELM in understanding the effects of some of our factors, we do not adhere strictly to this model.

3.5 Personal Relevance: Familiarity Breeds Trust

Prior works has also investigated the relation between familiarity of users with technology or specific things and its impact on trust and behaviour, though outside of an ELM context. Interestingly, Hoffman et al. found that concerns over secondary use of information were most pronounced for both those who were most and least likely to shop online [32]. However, the drivers for these groups may be different, with the concern for those who were most likely to shop online coming from more avenues of possible risk, while lack of familiarity was the cause leading to increased concern for those who tended to not shop online.

Other works have investigated overall Internet familiarity and relevance and their links to concern and trust. For example, van Schaik et al. found that those with less frequent Internet usage had higher perceptions of risks and threat [87]. Furthermore, overall Internet experience (in years) was found to be significantly correlated to security-preserving behaviours while the average amount of time spent on the Internet was not [87]. Jeske and van Schaik found similar results in that the length of Internet experience was indeed a significant predictor of familiarity with online threats as well as of online behaviour, though they also found that the time a user
spent on the Internet to be a significant predictor [33].

Personal relevance can also be evaluated with specific experiences related to the possible security and privacy issues at hand. Thus, the personal experiences and context, particularly negative security incidents, influence privacy behaviour [36, 15]. Some scholars have explicitly linked higher personal relevance to higher trust. For example, Harris et al. noted that users that had greater familiarity with finding, purchasing, or downloading apps had greater trust and less perceived risk [31]. In fact, the familiarity of an individual with the app ecosystem was a better predictor of trust than the perceived security of an app.

Therefore, the more personal relevance—whether through familiarity, expertise, or personal experience, an individual has to the issue—the better equipped they are to evaluate risks and the higher trust they have. This can be used to better understand the “technification” axis of cyber securitization, in that with more expertise, the better able people are to actually engage with the securitizing arguments and make informed decisions about whether to accept them. To our knowledge, this is first study to investigate relevance to an app by usage frequency of the specific app as impacts trust rather than general user traits such as familiarity with the app ecosystem, time spent online, or technical expertise.

3.5.1 Technical Background

We also look specifically at expertise and its relation to trust and behaviour through works that distinguish whether participants had a technical background. Although users with technical backgrounds and those without had generally different mental models of online threats and more awareness of threats from hackers, the government, and ISPs, Kang et al. did not find any direct relation between a technical background and the actions take to increase online security [36, 30]. Indeed, it is generally noted that though those with expertise may have more awareness of threats, the actual
behaviour of experts are not always different from that of lay users [2]. Therefore, expertise is not always directly correlated with behaviour, though it is relevant to perception of risk.

Furthermore, when distinguishing between those with expertise and those without, the user’s level of expertise must be considered in the way risk is communicated, so as to be able to persuade without overwhelming the recipient with information [2]. In fact, those without expertise further also sought out experts when confronted with previously unseen or insecure behaviours [15]. This is likely due to the fact that most users believe experts have a better understanding of risks [26]. This ties in neatly with the “technification” grammar of securitization, wherein interpretation of facts may be left to the experts, who then present the persuasive argument and thus are able to shape the narrative to their liking.
Chapter 4

Methodology

We ran an user study of 829 participants on Amazon Mechanical Turk to understand the persuasiveness of various elements present in securitizing narratives when used in arguments related to app data collection. We chose to use MTurk as the population’s responses are generally representative of the US population, apart from those over 50 [63]. It is further noted that MTurk workers’ responses about security and privacy behaviour and knowledge were found to be consistent across major news events (such as the 2014 Snowden leaks, the 2016 US presidential election, and the 2018 Cambridge Analytica news [63]. However, attitudinal responses, which we explored in this study, may vary.

4.1 Survey Design

The survey investigated three main factors, nationality, language, and government access to user data in arguments regarding app data collection on user perceptions of the app. Each of these factors was an independent variable in the construction of an argument presented to the user.

Firstly, nationality of the app was varied in that users either encountered an app that is owned by a Chinese company or one that is owned by an American company.
As the political and online discourse surrounding TikTok was the motivation for this study, we naturally selected TikTok as the Chinese app. For its American counterpart, we chose an app we felt was similar to TikTok in key aspects. To this purpose, we elected to use the Instagram app, an American social media app. Both apps are extremely popular, ranking consistently in the Top 10 free apps on the Apple Store since May 2020 [4]. Furthermore, both applications have over 1 billion monthly active users, of which consists 100 million monthly American users [16, 17]. Thus, respondents were either asked about and presented with arguments regarding the app TikTok, owned by Chinese company ByteDance, or Instagram, owned by American company Facebook. As one main axis of the securitizing moves regarding TikTok consisted of highlighting the fact that TikTok was owned by a Chinese company, we hypothesized that those who encountered an argument about TikTok would have less trust in the app after treatment.

**H1: Arguments concerning a non-American app are more persuasive.**

The second independent variable was that of language, which changed the tone of the argument presenting the information. There were two basic argument structures, one using more neutral language and one using more dramatic, alarming language. To simulate arguments that users may actually encounter about these apps, we took much of the wording and style in the alarmist condition from the viral Reddit comment stating the dangers of TikTok [80]. The text of the original comment is reproduced in Appendix A.2. For the neutral argument, we mimicked language, particularly around data collection, from that used in the privacy policies of TikTok and Instagram. However, in each case, the information presented regarding data collection and other entities that may have access to user data remained constant, though framed differently. As posited by the technification grammar of securitization in cyberspace, lay users may rely more on experts’ framing of the severity of any cyber issue to form their opinions due to their lack of confidence in their own abilities to parse the
technical details. Thus, the alarmist conditions used somewhat more technified language and further explicitly stated the data collection practices undertaken by the app were underhanded and generally dangerous. Therefore, despite the same facts about data collection being present, an alarming framing of the issue may increase alarm and thus also reduce trust. We hypothesized that the use of alarmist language in presenting an argument leads users to be less trustful of the application than a relatively neutral statement.

**H2**: Arguments using alarming language about an app are more persuasive.

Our third and final independent variable was the inclusion of claims of government access to user data collected by the app. Arguments with this variable present included additional statements that explicitly claimed that the government (Chinese or US depending on the application) may have access to data collected by the application. As Americans tend to be suspicious of government collection of data [39, 6], we expected lower levels of trust for those presented with the extra claim of government access to data. This variable in itself does not distinguish between possible different effects on trust between the US or the Chinese government but rather examines suspicions regarding either government.

**H3**: Arguments including alleged government access to user data collected by an app are more persuasive.

Furthermore, as Americans are wary not only of Chinese government access to user data, but also US government access to data, we wanted to specifically distinguish between alarm due to any government access to data, and alarm due to specifically Chinese government access to that same data. Therefore, we distinguish between the two apps, and posit two further hypotheses.
**H3a:** Arguments including alleged US government access to user data collected by Instagram are more persuasive.

**H3b:** Arguments including alleged Chinese government access to user data collected by TikTok are more persuasive.

The wording of the conditions between the two apps remained the same across conditions that were constant in their language variable, apart from words that varied due to the nationality of the app itself. Each of the three independent variables was either present or absent. Thus, there were 8 total conditions to which respondents were randomly assigned, shown in Table 4.1. The text of each condition can be found in Appendix A.1

<table>
<thead>
<tr>
<th>Condition Name</th>
<th>(Chinese) App Name</th>
<th>Alarmist Language</th>
<th>Government Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>TikTokAlarmistGovt</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TikTokNeutralGovt</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>TikTokAlarmistBase</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>TikTokNeutralBase</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>InstaAlarmistGovt</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>InstaNeutralGovt</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>InstaAlarmistBase</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>InstaNeutralBase</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 4.1: All eight conditions to which participants were randomized. Each of the three independent variables were either present or absent for each condition.

The breakdown of respondents to each condition are as follows: TikTokAlarmistGovt had 109, TikTokNeutralGovt had 107, TikTokAlarmistBase had 105, TikTokNeutralBase had 106, InstaAlarmistGovt with 101, InstaNeutralGovt with 100, InstaAlarmistBase with 100, and InstaNeutralBase with 101.

In order to understand how much personal relevance each user had to the application, the survey further collected information about whether the respondents have used the app, and if so, how often they did so. The scale for how often a respondent
used the app was inspired by the survey instrument used by Rosen et al. to measure social media use [68]. Before the treatment (i.e. before participants were presented with the argument), the survey asks respondents to rate how trustworthy they found the app on a 5-point Likert scale (from “Very untrustworthy” to “Very trustworthy”), either due to their own interactions with the app or what they have heard about it. It also asks how much data they believed the application to collect on a 5-point Likert scale (“Everything it can,” “Much more than necessary,” “As much as these types of apps generally do,” “Only what is necessary,” and “None”). They are then asked to read a short paragraph presenting information about the app, the contents of which differed depending on the condition. After the treatment, users are once again asked how much they trust the app, as well as how much data they believe was collected by the app using the same scales as the corresponding questions before the argument. The survey concludes with a few demographic questions.

We chose to ask both about trust in the app as well as about data collection because although trust and perceptions about data collection are highly correlated [47, 74, 32], we believed there may be a difference in trust even when the data believed to be collected remained the same depending on user beliefs regarding the recipient of that data. Furthermore, as the information presented regarding what the app gathered is the same across all eight conditions, data collection assessment was regarded as a way to measure differences between arguments when results should objectively be the same across conditions. Therefore, we hypothesized that because each argument included the same information about data collection, users would perceive the same amount of data was being collected across variables.

**H4a:** Data collection assessment after treatment is consistent across applications.

**H4b:** Data collection assessment after treatment is consistent across the tone of language used to present the argument.
**H4c:** Data collection assessment after treatment is consistent across arguments whether or not they contained claims of government access to user data.

We also included an open-ended textbox that asked users to state the nationality of the app they saw. This allowed us to see whether users were generally aware of the nationality of either the TikTok or Instagram apps (which are Chinese and American respectively). This question further served a dual purpose as an attention check to help us reduce the number of incoherent and random responses.

The full text of the survey presented to respondents can be found in Appendix A.1

### 4.2 Analysis Plan

To explore our research questions and while minimizing the amount of Type I (false positive) errors, we committed to an analysis plan. Although trust was collected as an ordinal variable, we converted it into numerical variables during analysis, with 1 representing “Very untrustworthy” and 5 representing “Very trustworthy”. For data collection assessment, we replaced “Everything it can” with 5 and “None” with 1. The specifics of analysis are detailed in the following sections.

#### 4.2.1 Statistical Tests to Evaluate the Effects of an Argument

We were interested in the way inclusion of various elements present in securitizing narratives surrounding TikTok affected the persuasiveness of arguments. We thus evaluated an argument’s persuasiveness by measuring whether there were significant decreases in each subject’s levels of trust for all subjects in a condition. Thus, an argument was deemed persuasive if a user’s trust in the app decreased after reading the argument, either going from believing the app was trustworthy to neutral, from being neutral to believing the app was untrustworthy, or from believing the app was untrustworthy to very trustworthy.
trustworthy to believing it was untrustworthy. These three broad categories were chosen as they encapsulated the general differences in attitude (positive, neutral, negative). We did not believe distinguishing between a shift from believing an app was “Very trustworthy” to “Somewhat trustworthy” was a large enough shift in opinion to warrant the user being marked as convinced because both of these trust levels still imply generally positive feelings towards the app. We used signed-rank tests to detect whether the changes in trust were significant as these tests are meant for paired data, which in this case were the trust levels before and after treatment for each user. As signed-rank tests check for within-unit differences, differences in how each user interpreted and evaluated trust would not heavily affect the result as the main goal was to understand changes in a user’s trust in the app. These statistical tests were further chosen as they are non-parametric, meaning we make no assumptions about distribution. The null hypothesis for a signed-rank test can be interpreted as testing whether the change in the variable of interest is symmetrically distributed around 0. In this context, this would mean that trust was as likely to increase as decrease after treatment. A significant p-value indicates that trust levels in the population experienced a consistent shift in one direction (becoming overall more or less trusting after treatment). We visualized the data and compared the median and mean trusts of the population before and after treatment to understand the direction of change. Should the general trend suggest a significant decrease in trust over the sample, then the argument was said to be persuasive.

We were further interested in the persuasiveness of arguments containing (or not containing) certain of our variables relative to each other. Thus, we ran pairwise comparison between arguments, and defined an argument (or arguments containing certain variables) as more persuasive than another if it persuaded a significantly higher proportion of users (to become less trustful of the app). Thus, we calculated the number of users that were and were not convinced by the argument in each
population we wished to compare and used Fisher’s exact tests to detect significance. Fisher’s exact tests are a non-parametric test, and thus we did not have to make any assumptions about normality of data distribution. These tests determined the likelihood that results as extreme as were observed occurred solely by chance, and thus the null hypothesis was that there was no difference in the outcomes of the two treatments. If there was a statistically significant difference between the populations, we examined the proportion of users that were persuaded in each population, and determined the argument that convinced a greater proportion of the subjects to be more persuasive.

However, the above definitions fail to distinguish the nuances between trust levels that fell into the same broad category (e.g. between “Somewhat untrustworthy” and “Very untrustworthy”). As there were likely differences between such responses, we used Mann-Whitney-Wilcoxon tests (also known as Mann-Whitney U tests or Wilcoxon rank-sum tests) to compare the overall trust level distributions pairwise between groups. MWW tests are, like all the tests we have chosen, non-parametric, and neither assume normality nor assume equal sample sizes. Through these tests, we were able to identify whether the distribution of responses between two populations were similar. Thus, we ran MWW tests on the trust levels between groups of interest before treatment to see if initial trust distributions were the same. We also used these tests after treatment to understand trends where resulting trust levels were significantly lower or when respondents were significantly more likely to find an app more untrustworthy. If, for two different conditions, initial trust level distributions were the same (as expected due to the random nature of assignment) but resulting trust distributions were not, then that reveals that the argument one condition had a different effect from another. This also allowed us to interpret results that included the users that distrusted an app before treatment, as a user that already believed an app was somewhat or very untrustworthy by our definition would not have been persuaded
by the argument, even if they believed an app was “Somewhat untrustworthy” before treatment and were convinced that it was “Very untrustworthy” after. As MWW tests do not state which group had a higher or lower trust, but rather that trust levels were different, we used data such as the median and mean trust levels of each group to draw conclusions about the overall distributions of trust levels in each population.

All of the statistical tests we chose suited the ordinal nature of our data. We do recognize that two-sample t-tests, which would test for a difference in means, were an alternative to Mann-Whitney-Wilcoxon tests in comparisons between samples. Indeed, for most distributions with enough samples, t-tests and their non-parametric equivalent MWW tests hold around the same power [88]. Similarly, we also considered paired t-tests in the place of signed-rank tests. Nevertheless, to best preserve the ordinal nature of our data, we decided upon the non-parametric tests, as we also did not want to make claims about the magnitude of differences in mean trust, as would be implicit in results from the paired and two-sample t-tests. However, due to these choices, the tests we used investigated the presence of change (in the case of the signed-rank test) or for differences in outcomes and distributions, but did not allow us to make explicit claims about the magnitude of change.

Thus, we supplemented these comparisons between groups by running ordinal logistic regression models to understand what factors and variables were best at predicting trust after treatment. In each model, we included the three independent variables as predictors, each of which were turned into indicator variables as predictors as follows:

- **Nationality**: 1 if app was TikTok, 0 if app was Instagram
- **Language**: 1 if the argument used alarmist language, 0 if it used neutral language
- **Government Data Access**: 1 if the argument included claims that data was shared with government, 0 if aforementioned argument was absent
The coding of indicator variables assigned 1 to the variables that were hypothesized to have negative effects (i.e. decrease trust) on user perceptions of the app. The $p$-values for each predictor in a model allowed us to understand whether said predictor was significant. However, we were most interested in the data from the odds ratio and from the predictions of the model. The odds ratio allowed us to understand how much more likely a user in a certain condition would find the app less (or more) trustworthy than a user in another condition, giving us some insight into the magnitude of certain predictors’ effects. Furthermore, using our regression models, we could predict the probabilities of individuals in any condition responding with each level of trust in the app, further revealing the impact of certain variables. In particular, we examined the likelihood of a user believing the app was “Very untrustworthy” or “Somewhat untrustworthy” and compared that across conditions.

Using all of the above methods, we hoped to gain a clear understanding of which factors made an argument persuasive to general users, and the extent of these effects.

4.2.2 Understanding the Effects of Our Independent Variables

**RQ1: What factors are effective in convincing users to be more distrustful of an app?**

To investigate our first research question, we divided our sample a few different ways by which of the three independent variables (app nationality, language, government data access) were present in the argument users read.

We first divided by condition, resulting in 8 samples that each saw a different argument. For each of these conditions, we ran signed-rank tests on trust before and after treatment to evaluate the persuasiveness of each message. We also fit an ordinal regression model to our data, with the outcome being trust after treatment.
and predictors being each of the three independent variables. We then looked at the predicted probabilities for each level of trust within each condition to get an overall sense of the effects of each argument.

We further investigated each of our three independent variables in turn by dividing our sample into two groups—those that contained the variable and those that did not. For example, when exploring the effects of app nationality, one group contained all the users that saw the TikTok app and the other those that saw Instagram. Similarly, to explore the effects of language, all users assigned to one of the four conditions with alarmist language were one group, and all those that read one of the four statements with neutral language were the other group. Thus, we compared all users assigned to a condition with TikTok against all users assigned to a condition with Instagram, all users assigned to a condition with alarmist language against all those with neutral language, and all users assigned to a condition with claims of government collection of data against all those assigned to one without.

To determine the effect of the presence of each independent variable in an argument, we compared the persuasiveness and resulting trust levels of those in conditions with said variable and those without. We first detected whether conditions with a certain variable were more persuasive through using Fisher’s exact tests to compare the number of users persuaded within each group. We then also ran Mann-Whitney-Wilcoxon tests comparing trust levels after treatment for those exposed to arguments containing a particular variable against those who were not, in order to detect differences in the final distributions of trust levels. Lastly, we examined the odds ratio and $p$-values for each of the variables from an ordinal logistic regression model with the three independent variables and predictors and post-treatment trust as the outcome. The odds ratio allowed us to determine how much more likely participants assigned to conditions with a certain variable were to find the app less trustworthy than those assigned to conditions without that variable, while the $p$-value determined
if the variable was significant in the model.

These tests and models all explored the effect of any singular independent variable, without accounting for interactions with the other two variables. Some of these interactions, particularly those related to the securitizing moves surrounding TikTok, were explored in the next research question.

**RQ2:** Are arguments more persuasive when they claim securitized actors have access to user data?

Firstly, we were interested in the effectiveness of claims that the government had access to user data without it necessarily being a foreign government. Thus, within each app (and thus with the same government), we compared the effectiveness and resulting trust levels of arguments that data was shared with the government against arguments without that claim. This allowed us to understand the effects of claims including government data access on users without assuming that claims that the US government had access to user data had the same effects as claims that the Chinese government had access to user data.

Of course, as we were also interested in whether the claims about the US government differed from claims about the Chinese government, we compared the conditions with such an argument (TikTokAlarmistGovt and TikTokNeutralGovt) with the corresponding conditions for Instagram (InstaAlarmistGovt and InstaNeutralGovt). We expected to see an especially strong interaction between nationality of app and claims of data sharing with the government. Thus, if the argument included claims that data was being shared with the government and the app was TikTok (non-American), we expected to see the lowest levels of trust. Through pairwise comparisons of these conditions by MWW tests with all else being held constant, we could understand whether the same claims of government data access were stronger when applied to a Chinese app and to the Chinese government than to an American app and the US government.
4.2.3 Perceptions of Data Collection

As all eight conditions included the same information in terms of data collection (i.e. what data was being collected and that the app collected more data than Reddit and Twitter), we decided the best way to understand this information was through pairwise comparisons of data collection assessment between groups. If the facts of all arguments were understood precisely the same way, we would expect to see no difference between any groups in their beliefs regarding the amount of data being collected by the app after treatment.

We first decided to look at differences in data collection assessment by our independent variables. Groups were divided in the same way as when evaluating the effects of each variable on trust, and we ran MWW tests to compare groups with and without a particular variable both before and after treatment.

We then also explored the perceptions of data collection in the specific conditions that mirrored one of the securitizing moves made about TikTok, namely claims of the Chinese government having access to user data. We expected a strong interaction between the presence of government and nationality of the app. We thus investigate whether it was merely awareness of government access to data that was alarming to users, or whether it was the suspicion of the recipient of the data that sparked distrust. We ran MWW tests on both data collection and trust levels between TikTok and Instagram in conditions where a government was claimed to have access to user data. As the information regarding what data was being collected remained consistent across apps, we hypothesized that the amount of data perceived to be collected would be similar whether users saw TikTok or Instagram. However, we also hypothesized participants encountering an argument regarding TikTok (and thus a Chinese company) and (Chinese) government access to data would have lower levels of trust than the corresponding condition for Instagram due the additional implication of foreign (rather than the respondent’s own) government having access to data.
**H5**: Data collection assessment after treatment is consistent across arguments that contain claims of government access to user data, with less trust when this data is believed to be going to a securitized actor.

### 4.2.4 Effects of App Usage/Personal Relevance

Our third research question explored the amount of personal relevance the app had to an user and its effect on argument persuasiveness.

**RQ3**: Are those with high personal relevance to an application less persuaded by negative arguments towards the app?

We measured personal relevance to an app by how often respondents used said app. We hypothesized that users with high personal relevance (indicated through higher usage of the app) were less likely to find any arguments persuasive than those with lower personal relevance [62]. Users were divided in two main ways. The initial division was between those who had previously used the app, and those who had not. However, this assumed that those who have used the app were all similar, regardless of frequency of use. Thus, we further divided the group who had used the app into two smaller subgroups, high usage and thus high personal relevance (i.e. those who answered “Several times a day” or more often when asked about the frequency with which they used the app), and those with low usage and thus only some personal relevance (those who used the app at most once a day). The division at “Several times a day” was chosen because both apps (TikTok and Instagram) are social media apps, which often necessitate relatively frequent checking of the app. Indeed, on average, US TikTok users opened the app 8 times a day [16].

**H6**: Arguments are more persuasive to those with lower personal relevance to the app.
Within each group, we ran signed-rank tests to see whether the argument was persuasive and there were significant changes in trust for each user. We also tested whether arguments were more effective to those who had not used the app against those who had, as well as whether they were more effective for low frequency users than high frequency ones. We also conducted MWW tests on trust after treatment between the groups to compare whether there were significant differences in trust, expecting higher distributions of trust for those who had higher relevance to the app.

The above tests assume that personal relevance affected TikTok and Instagram users the same way. To explore whether app usage did in fact moderate any effects of the app itself, we further split the above groupings by app. We then ran pairwise tests between TikTok and Instagram users (and non-users) within each relevance category (users, non-users, high frequency users, and low frequency users), looking at distributions trust before and after treatment as well as the persuasiveness of the argument. This allowed us to understand whether individuals with similar app usage were similar in initial trust and similarly affected by arguments, regardless of app.

We also fit an ordinal regression model that accounted for personal relevance, using as predictors each of the three independent variables as well as the frequency with which someone used the app. We mapped responses regarding frequency app usage to a scale from 0 to 10, with 0 being those who have not used the app, and 10 being those who reported using the app “All the time.” On this scale, those who used the app at least “Several times a day” and thus were classified as high usage individuals were at 7 or higher on this numeric scale. The resulting odds ratio gave us the likelihood of finding the app more trustworthy than those who used the app less with each unit increase in app usage frequency.
4.2.5 Demographic Effects

We concluded our analysis by looking at the relation between background and demographic factors and the effects of various arguments. The variables of note were the self-reported social and economic leanings of the respondents, as well as whether they had a technical background. We asked respondents to rate their political views on social issues and on economic issues on a 5-point Likert scale from very liberal to very conservative. Technical background was coded as a 0-1 indicator variable. To measure their effects, we fit an ordinal regression model using our three independent variables, frequency of app usage, and each of the aforementioned background variables as predictors for trust after treatment. Through the $p$-values, we were able to see the strength of each predictor, while the odds ratio allowed us to understand the direction of its effect.

We hypothesized that those with technical backgrounds, due to their ability to more objectively parse the information presented in the arguments, would both have higher trust levels than those without a technical background, and not have different trust levels between apps.

\textbf{H7a}: Arguments are more persuasive to those without a technical background.

\textbf{H7b}: Arguments about TikTok and Instagram are similarly persuasive to those with a technical background.

To this end, we ran MWW tests on trust both before and after treatment between those with and without technical backgrounds. We further divided those with technical backgrounds into those randomized to TikTok and those randomized to Instagram, and compared the pairwise distributions of trust before and after treatment between apps.
4.2.6 Corrections for Type I Errors

As we ran a multitude of statistical tests, we elected to use the Benjamini-Hochberg correction to control for the false discovery rate. Thus, using this correction, the proportion of null hypotheses rejected that should not have been would not exceed 0.05.
Chapter 5

Results

We received responses from 941 users on MTurk, of which 829 were analysed and the rest discarded due to incoherent answers. Of these 829, 109 were in the TikTokAlarmistGovt condition, 107 in TikTokNeutralGovt, 105 in TikTokAlarmistBase, 106 in TikTokNeutralBase, 101 in InstaAlarmistGovt, 100 in InstaNeutralGovt, 100 in InstaAlarmistBase, and 101 in InstaNeutralBase. The demographic breakdown of our respondents were as follows: 6.0% were between the ages of 18-24, 42.0% between 25-34, 29.0% between 35-44, 16.6% between 45-50, 6.2% between 60-74, and 0.2% over 75. We analysed the responses based on our analysis plan, finding significant evidence of the persuasiveness of each argument, differences in the effects of variables present in the arguments, as well as a relationship between the personal relevance users had to an app and how persuasive they found arguments relating to said app.

5.1 Effects of Arguments

We first analysed whether the treatment, i.e. presenting the user with an argument regarding a mobile application, was able to significantly decrease trust in the app. As stated in our Methodology section (Section 4), an argument was deemed persuasive if it decreased user trust from 5 or 4 (“Very trustworthy” and “Somewhat trustwor-
### Table 5.1: Mean and medians for how trustworthy users found an app before and after presented with the argument from each condition. Lower numbers indicate lower trust. The $p$-values result from signed-rank tests for persuasiveness of argument. The $n$ column denotes the number of respondents in each condition.

<table>
<thead>
<tr>
<th>Condition</th>
<th>$n$</th>
<th>Mean Trust Before</th>
<th>Mean Trust After</th>
<th>Median Trust Before</th>
<th>Median Trust After</th>
<th>$p$-val</th>
</tr>
</thead>
<tbody>
<tr>
<td>TikTokAlarmistGovt</td>
<td>109</td>
<td>3.06</td>
<td>1.73</td>
<td>3</td>
<td>1</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>TikTokNeutralGovt</td>
<td>107</td>
<td>3.02</td>
<td>1.97</td>
<td>3</td>
<td>1</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>TikTokAlarmistBase</td>
<td>105</td>
<td>3.03</td>
<td>1.94</td>
<td>3</td>
<td>2</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>TikTokNeutralBase</td>
<td>106</td>
<td>2.86</td>
<td>2.01</td>
<td>3</td>
<td>2</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>InstaAlarmistGovt</td>
<td>101</td>
<td>3.67</td>
<td>2.11</td>
<td>4</td>
<td>2</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>InstaNeutralGovt</td>
<td>100</td>
<td>3.61</td>
<td>2.16</td>
<td>4</td>
<td>2</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>InstaAlarmistBase</td>
<td>100</td>
<td>3.55</td>
<td>2.25</td>
<td>4</td>
<td>2</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>InstaNeutralBase</td>
<td>101</td>
<td>3.49</td>
<td>2.56</td>
<td>4</td>
<td>2</td>
<td>&lt; 0.001</td>
</tr>
</tbody>
</table>

Figure 5.1: Perceived trustworthiness of the app in each condition. Lower numbers indicate lower trust.
thy”) to 3 (“Neither trustworthy nor untrustworthy”) or below, or from 3 (“Neither trustworthy nor untrustworthy”) to 2 or 1 (“Very untrustworthy” and “Somewhat untrustworthy”). Due to the ordinal nature of the data, we ran Wilcoxon signed-rank tests to detect differences in trust that had consistent trends in one direction (i.e. a general increase or decrease). As all eight of the arguments were intended to decrease the user’s trust in an app, we expected to see higher mean and median levels of trust before users were presented with the paragraph. The results can be found in Table 5.1.

In all 8 conditions, respondents’ trust in the app collectively significantly decreased after treatment ($p < 0.001$), showing that all arguments were persuasive. As trust was collected as ordinal data points through a Likert scale, the magnitude of change of trust levels could not be accurately reflected through a difference in means, though they helped to understand the direction of change. As expected, the mean and median trust decreased in all conditions, with six out of eight conditions having a median trust of 2 (“Somewhat untrustworthy”) after treatment, and the two conditions most related to the securitizing narrative surrounding TikTok (TikTokAlarmistGovt and TikTokNeutralGovt) having a median trust of 1 (“Very untrustworthy”), the lowest level possible. A visual representation can be found in Figure 5.1.

To understand the overall effects of arguments in each condition, we ran an ordinal logistic regression, with the predictors being the three independent variables used in constructing the argument (nationality of app, type of language used, and whether claims of government access to data were present). We focused on examining which arguments resulted in higher probabilities of the user deeming the app either “Somewhat untrustworthy” or “Very untrustworthy”. The predicted probabilities of users falling into each trust level are found in Table 5.2. We can see that the condition with all three independent variables present resulted in a group with the highest likelihood of finding the app untrustworthy, with respondents in said condition over 20% more
Table 5.2: Predicted probabilities (rounded to the nearest thousandths) of how trustworthy someone would find an app after presented with the argument from each condition using an ordinal regression model. Total untrust. column is the sum probability a user would find the app either very or somewhat untrustworthy.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>TikTokAlarmistGovt</td>
<td>109</td>
<td>0.549</td>
<td>0.272</td>
<td>0.079</td>
<td>0.075</td>
<td>0.024</td>
<td>0.821</td>
</tr>
<tr>
<td>TikTokNeutralGovt</td>
<td>107</td>
<td>0.490</td>
<td>0.294</td>
<td>0.094</td>
<td>0.092</td>
<td>0.031</td>
<td>0.784</td>
</tr>
<tr>
<td>TikTokAlarmistBase</td>
<td>105</td>
<td>0.473</td>
<td>0.299</td>
<td>0.098</td>
<td>0.097</td>
<td>0.033</td>
<td>0.772</td>
</tr>
<tr>
<td>TikTokNeutralBase</td>
<td>106</td>
<td>0.415</td>
<td>0.313</td>
<td>0.113</td>
<td>0.118</td>
<td>0.041</td>
<td>0.728</td>
</tr>
<tr>
<td>InstaAlarmistGovt</td>
<td>101</td>
<td>0.397</td>
<td>0.316</td>
<td>0.118</td>
<td>0.125</td>
<td>0.044</td>
<td>0.713</td>
</tr>
<tr>
<td>InstaNeutralGovt</td>
<td>100</td>
<td>0.342</td>
<td>0.320</td>
<td>0.132</td>
<td>0.150</td>
<td>0.055</td>
<td>0.662</td>
</tr>
<tr>
<td>InstaAlarmistBase</td>
<td>100</td>
<td>0.327</td>
<td>0.320</td>
<td>0.136</td>
<td>0.158</td>
<td>0.059</td>
<td>0.647</td>
</tr>
<tr>
<td>InstaNeutralBase</td>
<td>101</td>
<td>0.277</td>
<td>0.314</td>
<td>0.149</td>
<td>0.186</td>
<td>0.073</td>
<td>0.594</td>
</tr>
</tbody>
</table>

5.2 Effects of Independent Variables

From the signed-rank tests of trust by each condition, we know that all arguments were broadly persuasive. We thus now compare the persuasiveness of each independent variable present in the arguments through pairwise comparisons between all arguments containing a certain variable against all those that did not (4 for each group). This was determined by Fisher’s exact tests of the number of users persuaded by arguments when the variable was present against those persuaded by arguments without the variable. Thus, arguments in one group were deemed more persuasive if there was a statistically greater number of users persuaded than corresponding arguments in the other group.

Finally, to compare overall distributions, including those who were initially distrustful of the app, we ran Mann-Whitney-Wilcoxon tests to compare trust levels
Table 5.3: Mean and medians for how trustworthy users found an app before and after presented with an argument containing or not containing each variable. Lower numbers indicate lower trust. The \( p \)-values under trust result from MWW tests of trust distributions between conditions with and without the variable. The rightmost \( p \)-value comes from Fisher’s exact tests of the number of users persuaded by the argument or not. The \( n \) column denotes the number of respondents in each condition.

<table>
<thead>
<tr>
<th>Variable</th>
<th>( n )</th>
<th>Trust Before</th>
<th>Trust After</th>
<th>Persuaded</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Mean</td>
<td>Med.</td>
<td>( p )-val</td>
</tr>
<tr>
<td>Nat’lity</td>
<td>Yes</td>
<td>427</td>
<td>2.99</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>402</td>
<td>3.58</td>
<td>4</td>
</tr>
<tr>
<td>Lang.</td>
<td>Yes</td>
<td>415</td>
<td>3.32</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>414</td>
<td>3.23</td>
<td>3</td>
</tr>
<tr>
<td>Govt</td>
<td>Yes</td>
<td>417</td>
<td>3.33</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>412</td>
<td>3.22</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 5.4: Odds ratios and \( p \)-values for each of the three independent variables present in the argument as predictors in an ordinal regression model. Each predictor was processed as a 0-1 indicator variable.

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Odds Ratio</th>
<th>( p )-val</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nationality</td>
<td>0.541</td>
<td>(&lt; 0.001)</td>
</tr>
<tr>
<td>Language</td>
<td>0.788</td>
<td>0.063</td>
</tr>
<tr>
<td>Government Access</td>
<td>0.738</td>
<td>0.018</td>
</tr>
</tbody>
</table>

Since trust in an app was collected as ordinal data, we also ran ordinal regressions to evaluate the effect of each argument by predicting trust levels after treatment. Each of the three independent variables used in constructing the argument were used as predictors, represented as a 0-1 indicator variable. This model provided a further way to evaluate the effect of any independent variable by looking at the likelihood of a user finding a condition with the variable present more untrustworthy than one without. Results from this regression model can be found in Table 5.4.
5.2.1 App Nationality

The main variable of interest to us was the nationality of the app, varied through which app the respondent saw. We hoped to understand whether app nationality was an effective signal in decreasing trust by comparing the responses of all users randomized to TikTok (a Chinese app) against those randomized to Instagram (an American app) both before and after treatment. The results are given in Table 5.3, where “Yes” for “Nat’lity” indicates that the respondent saw TikTok and “No” means the respondent saw Instagram. Both before and after being presented with the argument, users who saw the TikTok app found it significantly less trustworthy ($p < 0.001$) than those who saw the Instagram app.

Neither of the other two independent variables had significant differences in the distribution of preheld trust, as was expected from the randomization of users to conditions. We do note, however, that the app is the only one of our independent variables that users were exposed to before treatment, and therefore the only one that may impact initial trust levels. As trust in TikTok was lower than trust in Instagram even before being presented with an argument, users already had preconceived beliefs regarding each of the apps. Therefore, as 91.8% of people assigned to Instagram correctly answered that it was an American app/owned by a US company and 93.0% of people assigned to TikTok correctly answered that it was a Chinese app/was owned by a Chinese company, this supports the idea that nationality of the app deeply influenced trust in the app even before any attempt at persuasion was made.

We found no evidence to support H1 as the Fisher’s exact tests found that arguments concerning Instagram were more effective (i.e. caused more users to decrease their trust levels significantly) than those about TikTok. We hypothesized this may be due to the lower distributions of initial trust for TikTok, and explored this further in the section below.
Figure 5.2: Perceived trustworthiness of TikTok and Instagram after treatment by how trustworthy the user rated the app before treatment. Lower numbers indicate lower trust.

**Controlling for Differences in Preheld Trust between Apps**

As users’ initial trust in each of the apps differed significantly before being presented with the argument, we thus explored changes in trust for each app conditioned on trust in the app before treatment. As shown in Figure 5.2, although there was not much change in trust for those who were already distrusting of either app (i.e. believed app was very or somewhat untrustworthy before treatment), the distribution of trust after treatment appeared lower for those who saw TikTok than those who saw Instagram in higher trust categories (though this was not statistically significant through MWW tests).

To understand the results that showed arguments about Instagram were more persuasive, we compared the effectiveness of arguments about these two apps conditioned on initial trust levels. In other words, we compared the effectiveness of arguments for TikTok and Instagram within respondents who held each level of trust for either app before treatment. As by our definition, those who already distrusted an app could
Table 5.5: This table shows the number of users \((n)\) that fell into each level of trust in the app before treatment. Within each trust level, it then shows the mean trust between apps after treatment with \(p\)-values from MWW tests. It further shows the proportion of users persuaded, with the \(p\)-value resulting from Fisher’s exact tests.

<table>
<thead>
<tr>
<th>Initial Trust</th>
<th>(n)</th>
<th>Mean Trust After TikTok</th>
<th>Mean Trust After Insta.</th>
<th>Persuaded TikTok</th>
<th>Persuaded Insta.</th>
<th>(p)-val</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very untrust.</td>
<td>51</td>
<td>1.14</td>
<td>1.07</td>
<td>NA</td>
<td>NA</td>
<td>0.330</td>
</tr>
<tr>
<td>Some. untrust.</td>
<td>102</td>
<td>1.34</td>
<td>1.66</td>
<td>NA</td>
<td>NA</td>
<td>0.066</td>
</tr>
<tr>
<td>Neither</td>
<td>114</td>
<td>1.89</td>
<td>1.92</td>
<td>77.2</td>
<td>74.2</td>
<td>0.628</td>
</tr>
<tr>
<td>Some. trust.</td>
<td>120</td>
<td>2.43</td>
<td>2.36</td>
<td>75.8</td>
<td>78.8</td>
<td>0.451</td>
</tr>
<tr>
<td>Very trust.</td>
<td>40</td>
<td>2.9</td>
<td>3.18</td>
<td>60</td>
<td>50</td>
<td>0.330</td>
</tr>
</tbody>
</table>

not be further persuaded, we excluded those populations from this analysis. We also ran MWW tests on the resulting trust when conditioned by initial trust. Results can be found in Table 5.5.

We found that when grouped by initial trust levels, users that saw TikTok and those who saw Instagram were influenced similarly by arguments. In spite of consistently lower mean trust levels (Table 5.5) and visually lower levels of trust (Figure 5.2) for TikTok than Instagram, there were no statistically significant differences in how persuasive arguments were, nor was there strong evidence of differences in distribution by trust categories. However, we did note that the proportion of respondents who distrusted TikTok even before treatment was substantially higher, with over one-third of users (35.8%) finding TikTok somewhat or very untrustworthy compared with 16.7% of those who saw Instagram. This difference is backed up by the difference in initial trust revealed by the MWW tests across apps.

Despite the lack of statistical evidence for differences in argument effect between the two apps when conditioned on trust, we believed the pre-existing group that distrusted TikTok was important to consider. We hypothesize that the group which initially distrusted TikTok either were convinced due to repeated media exposure to claims that TikTok was untrustworthy, or were convinced specifically by the securitizing moves present in the media stories surrounding TikTok. However, given the
set-up of this study, we are unable to distinguish between these avenues of prior persuasion. This difference in initial levels of distrust between apps discussed further in Section 6.1.

We also explored the overall distribution of trust levels by app after treatment, wherein we found significant differences between those who saw TikTok and those who saw Instagram. Although median trust was same between the two groups, at “Somewhat untrustworthy,” the mean trust was lower for those presented with TikTok as compared to Instagram. Furthermore, a higher percentage of respondents found TikTok “Somewhat untrustworthy” or “Very untrustworthy”. Thus, there existed higher overall distrust for TikTok both before and after treatment.

From our ordinal regression, the app that users saw was the strongest predictor of trust post-treatment. Respondents who saw TikTok were 85% more likely to find the app more untrustworthy than those who saw Instagram when the other two independent variables were held constant (Table 5.4). This difference was statistically significant, with $p < 0.001$. We further see from Table 5.2 that in all cases with other variables held constant, users were markedly more likely to find TikTok “Very untrustworthy” or “Somewhat untrustworthy” than Instagram.

Thus, it is likely that overall, users do tend to hold less trust for TikTok over Instagram. However, as a much greater proportion of those who saw TikTok already believed it was untrustworthy, they by our definition could not be further persuaded and thus did not appear in our analysis of persuasiveness.

Furthermore, due to the prevalence of Sinophobia and the virality of arguments claiming TikTok was untrustworthy, it is possible that the population that was predisposed to believe such claims already formed these beliefs about TikTok, as evidenced by the much higher proportion of those who had low initial trust in the app. As most users (99.8%) either already used TikTok or have heard of TikTok, the lower number of users that initially trusted TikTok and those that initially trusted Instagram re-
vealed possible effects of negative media coverage of TikTok surrounding the ban in 2020. However, as the study was run months after the proposed ban and the height of the claims regarding TikTok’s ties to the Chinese government, it appears that such arguments were persuasive in the long-term to a significant number of users, resulting in lasting attitude change. Using the elaboration likelihood model to understand this phenomenon, the users that initially distrusted TikTok likely processed arguments using the central route, carefully considering the claims, and thus resulted in long-term change in their views of TikTok [62]. The remaining users probably also encountered similar arguments about TikTok through media and daily life, but they did not result in lasting attitude changes. Thus, the remaining population were similar across the two apps, and therefore processed arguments about the apps roughly the same and were similarly convinced by the arguments.

5.2.2 Use of Language

To understand if the tone of language used in presenting an argument affected effectiveness of the argument, we ran our pairwise tests comparing arguments that used different types of language. Thus, we compared responses in the conditions with language that was more alarmist and sensationalist (TikTokAlarmistGovt, TikTokAlarmistBase, InstaAlarmistGovt, and InstaAlarmistBase), much of which was modeled after the viral Reddit comment denouncing TikTok, against those with relatively neutral language (TikTokNeutralGovt, TikTokNeutralBase, InstaNeutralGovt, and InstaNeutralBase). Alarmist language is denoted with a “Yes” by language, and neutral language by a “No” by “Lang.” in Table 5.3. As expected, due to the randomization of respondents to conditions, there was no significant difference in trust levels before treatment.

We did not find conclusive evidence to support H2. Interestingly enough, though a higher proportion of users were persuaded by more alarmist arguments, the difference
was not statistically significant. However, there was a significant difference in distribution of trust levels after treatment between the group that read arguments using alarmist language against those that encountered arguments with neutral language ($p = 0.029$). Those who read an argument with alarmist language had lower trust levels, and more respondents in these conditions rated the app untrustworthy after.

From our ordinal regression model using the three independent variables as predictors, those presented with an argument that used alarmist language were $1.27$ times as likely to find the app more untrustworthy than those who were presented with an argument using neutral language (Table 5.4). However, this difference is not statistically significant in this model, with $p = 0.063$. When all other variables held constant, we also see increased probability of finding an app untrustworthy when alarming language was used (Table 5.2).

These results lead us to believe that although the tone of the argument was generally persuasive, its effects were generally outweighed by the other variables. Due to the difference in trust levels post-treatment but no evidence of alarmist arguments being more persuasive, we further theorize that perhaps arguments using alarming language were similarly persuasive as ones using neutral language, but caused greater decreases in trust.

### 5.2.3 Alleged Government Access to Data

The third of our three independent variables in the argument involved the addition of a claim that the government having access to the data an app was collecting. Depending on the nationality of the app, the government in question was either the US government or the Chinese government. We ran pairwise tests based on whether participants saw such a claim, comparing responses in the conditions with this claim (TikTokAlarmistGovt, TikTokNeutralGovt, InstaAlarmistGovt, and InstaNeutralGovt) against those without (TikTokAlarmistBase, TikTokNeutralBase, and InstaNeutralGovt).
InstaAlarmistBase, and InstaNeutralBase). Information regarding arguments including the claim of government access to data appear in the row with a “Yes” by “Govt,” and arguments without said claim are in the row labelled “No” in Table 5.3. There was no difference in trust between the two groups before being presented with the argument, which was expected given the random nature of assignment to conditions.

We found strong evidence to support H3, as arguments that stated that a government may have access to user data were much more effective than those without such claims ($p < 0.001$). There was also a significant difference in distribution of trust after treatment ($p = 0.012$), with those encountering arguments that included the claim of government data access on average having lower trust and with a lower proportion of respondents rating the app trustworthy. Thus, when users believe there is a possibility of government access to data, they become less trusting of an app, regardless of which government, making these claims quite effective in decreasing trust of an application.

As seen in Table 5.4, fears of government access to user data was also significant in our ordinal regression model ($p = 0.018$). Those presented with an argument that claimed a government may have access to their data were 1.35 times as likely to find the app more untrustworthy than those who did not see such a claim. When all other variables were held constant, the presence of claims of government access to data decreased the probability of finding the app trustworthy (Table 5.2).

### 5.3 Interactions Between Factors

#### 5.3.1 Government Access to Data

We further explored the effects of claims that a government had access to data by comparing both conditions with these claims for each app against the two conditions without these claims for the same app. We ran Mann-Whitney-Wilcoxon tests on the
Our results gave strong evidence to support H3a. For Instagram, respondents presented with claims of US government access to data had lower levels of trust than those without ($p = 0.023$). In addition, such an argument was better in persuading users to be less trustful of Instagram ($p = 0.004$), with 66.7% of users being persuaded when seeing such claims, compared with 52.2% of those who did not. This aligns with general American distrust of government data collection [6].

There was mixed evidence to support H3b in that there was no significant difference between trust levels of those who encountered an argument that the Chinese government may have access to data collected by TikTok and those who did not ($p = 0.087$). Despite the lack of statistical significance, it is worth noting that the mean and median trust levels were lower for those who encountered these arguments. There was, however, a difference in the persuasiveness of the argument ($p = 0.012$). 53.7% of those who encountered the claims that the Chinese government had access to TikTok data became less trustful of the app, compared with 41.2% of those who did not. This implies that while explicit claims that the Chinese government de-
increased trust more effectively than claims without, perhaps due to pre-existing views regarding TikTok’s lack of trustworthiness, the overall final trust distributions did not significantly differ.

These claims may have had less impact on overall trust for TikTok than Instagram due to the nationality of the app having a stronger effect than claims of government access to data, particularly if users already held preconceived notions due to previous exposure to similar arguments about TikTok through media and daily life. As the vast majority of users who encountered TikTok had heard about or used the app (99.8%), they may have already have encountered arguments that the Chinese government accesses TikTok user data, whereas users may not have previously explicitly associated Instagram’s data collection with the US government.

5.3.2 Securitization

We also investigated the effects of arguments specifically claiming that TikTok was a national security threat due to its alleged sharing of American user data with the Chinese government. As this type of claim was one of the main securitizing moves in the narrative surrounding TikTok, we believed these claims would be the most effective in reducing trust in an app. This particular framing of arguments appeared in the two conditions TikTokAlarmistGovt and TikTokNeutralGovt, both of which include claims that TikTok, being a Chinese app and possibly sharing data with the Chinese government, threatens US national security. To quantify this, we ran Mann-Whitney-Wilcoxon tests comparing the trust of users after being presented with these arguments of those randomized to TikTok against those randomized to Instagram, with language, the last variable, being held constant. We then combined both conditions containing claims of TikTok as a national security threat against both conditions where the argument claimed Instagram may be sharing data with the US government. Due to the different initial trusts between apps (discussed in Section 5.2.1), we chose
not to look at persuasiveness of the argument but rather only compare the resulting distributions. We further chose not to control for preheld trust as the smaller number of users by condition would not give us enough power.

There were significant differences in all three analyses. In conditions with neutral language (TikTokNeutralGovt vs InstaNeutralGovt), users who read an argument about TikTok had significantly lower levels of trust than those who read the same argument about Instagram ($p = 0.028$). Similarly, in conditions with alarmist language, (TikTokAlarmistGovt vs InstaAlarmistGovt), those who saw TikTok were less trustful of the app ($p = 0.007$). Lastly, when combining conditions with these specific securitizing arguments claiming Chinese government access to user data, compared to conditions with only government presence (TikTokNeutralGovt and TikTokAlarmist-Govt vs InstaNeutralGovt and InstaAlarmistGovt), this trend still held, with those who had seen an argument about TikTok having less trust ($p < 0.001$). In addition, those assigned to the conditions explicitly stating the Chinese government had access to user data were more likely to find the app untrustworthy than any other conditions (Table 5.2 and Figure 5.3).

However, these results of lower resulting overall trust may have been due to the lower levels of initial trust in TikTok. Nonetheless, we note that the resulting median trust for the conditions with TikTok was always at “Very untrustworthy,” the lowest possible value. We also note that there were no differences in the resulting trust distributions when comparing arguments with Chinese government data access against those without for TikTok alone, though there was a difference between TikTok and Instagram. This implies that there is indeed an extra factor causing less trust in an app when the government stated to have access to user data is a foreign government, though this warrants further investigation.
Table 5.6: Mean and medians for how much data users believed an app was collecting before and after presented with the argument containing or not containing each variable. Higher numbers indicate more data believed to be collected. The \( p \)-values result from MWW tests for differences in respondents’ assessment of data collection in all conditions with arguments containing one variable against all those that did not contain the variable.

5.4 Assessment of Data Collection

Parallel to our analysis of trust, we also analysed how much data users believed the app collected, on a 5-point Likert scale. As all 8 conditions stated that the same pieces of data were being collected (e.g. contact information, phone hardware, other installed apps etc.) though wrapped in different language depending on condition, we used data collection assessment as a metric to understand how user perceptions may differ even when the underlying facts presented were the same. Thus, we compared data collection assessment pairwise across the presence and absence of our three independent variables using Mann-Whitney-Wilcoxon tests. The results are seen in Table 5.6 and Figure 5.4.

Our results did not show support for H4a. Much like trust, data collection assessment differed significantly by nationality of the app (i.e. whether a user saw TikTok or Instagram). Even before reading the argument, users assigned to TikTok believed the app collected more data than users assigned to Instagram did (\( p = 0.023 \)), though the medians were the same for both groups. After treatment, the effect becomes clearer (\( p < 0.001 \)), with the median amount of data believed collected by TikTok to be 5 (“Everything it can”) while the median amount for Instagram remained at 4 (“Much
Figure 5.4: Boxplots of assessments of data collection by condition before and after treatment. Higher numbers indicate more data is believed to be collected by the app. Horizontal bars show medians, and boxes denote the interquartile range.
more than necessary”). However, the facts given specifically regarding data collection were exactly the same in both conditions, with only the names and nationalities of the apps changed, and in the case of those randomized to a condition with the government access variable, the government with which that data may be shared. Therefore, there were likely existing biases towards TikTok that were expressed not only in lower trust, but also in higher amounts of perceived data collection. As one of the securitizing moves regarding TikTok was related to claims of unnecessary and dangerous data collection [80], further compounded by the claims that this data was being shared with a foreign government [83], it thus makes sense that initial views of data collection differed between apps, particularly if the difference in preheld views were due to a population that had already been convinced to be wary of TikTok before the study. The more pronounced differences in data collection assessment after treatment may have been in part due to the differences in perceptions before treatment. However, there may have been some further amplifying effects of the app being TikTok, which had been accused in the public eye of suspicious and unnecessary data collection by a multitude of actors.

We found mixed evidence to support H4b. When analysing by the language variable, there were no significant differences in how much data was believed to be collected by the app, either before or after treatment. However, though the difference in the amount of data users believed the app collected post-treatment was not statistically significant between users that read an alarmist and a neutral argument ($p = 0.073$), it is worth noting that the medians differed. Those who saw an argument with alarmist language had a median of 5 (that the app collects “Everything it can”) while those presented with a neutrally-worded argument had a median of 4 (the app collects “Much more than necessary”). This is likely due to the fact that the alarmist condition words the argument in such a way that makes the data collection seem much more threatening and personally harmful to the user, such as saying the app
“is a data collection service that is thinly-veiled as a social network.” Furthermore, as the language variable was designed in part to understand the effects of the “technification” aspect of cyber securitization, alarmist language may have influenced users to not as carefully consider the specific pieces of data the app was said to collect (“information such as phone hardware, the other apps you have installed, and everything network-related”), but rather based their assessments on the assumption that the app was collecting as much data as possible due to the alarming wording framing the data collection.

There was strong support for H4c as the presence or absence of claims that a government may have access to data collected by the application had no effect on the amount of data users believed the app to collect. As expected, there was no difference in data collection assessment before users encountered the argument ($p = 0.238$), due to the random assignment to conditions. There was also no difference after users encountered the argument when compared across the government presence variable ($p = 0.265$), with medians being the same.

5.4.1 Lower Trust Due to Recipient of Data

We found strong evidence to support H5, that even though data collection assessment post-treatment was similar between apps when a government was said to have access to user data, the levels of trust varied. Indeed, though in all three of the pairwise analyses (comparing TikTokNeutralGovt, TikTokAlarmistGovt, InstaNeutralGovt, and InstaAlarmistGovt) in Section 5.3.2, there was a significant difference in trust levels between TikTok and Instagram, MWW tests on the amount of data users believed the app to collect did not differ in any of these analyses. Thus, although user may think TikTok and Instagram were empirically behaving the same in terms of their data collection practices in these conditions, they had different interpretations of and alarm levels regarding these actions, which was revealed through the differences
Table 5.7: Mean trust in an app, before and after being presented with the argument, sorted by personal relevance to the app. The “Yes” category includes all users who have used the app and the “No” category those who have not. The “High” frequency category includes those who use the app several times a day or more, and the “Low” usage category consists of those who use the app at most once a day. Lower numbers indicate lower trust. The leftmost p-values result from sign tests for argument persuasiveness. The second p-values compares trust levels pairwise between conditions. The final columns look at the percentage of users persuaded within each category.

<table>
<thead>
<tr>
<th>App Usage</th>
<th>n</th>
<th>Mean Trust</th>
<th></th>
<th>Persuaded</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Before</td>
<td>After</td>
<td>p-val</td>
<td>p-val</td>
</tr>
<tr>
<td>Yes</td>
<td>650</td>
<td>3.45</td>
<td>2.25</td>
<td>&lt; 0.001</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>179</td>
<td>2.64</td>
<td>1.50</td>
<td>&lt; 0.001</td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>277</td>
<td>3.84</td>
<td>2.69</td>
<td>&lt; 0.001</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>373</td>
<td>3.16</td>
<td>1.92</td>
<td>&lt; 0.001</td>
<td></td>
</tr>
</tbody>
</table>

in trust levels. Therefore, as none of the conditions varied the facts of data collection, it is likely not data collection alone that caused alarm, but the recipient of that user data also factored into evaluations of trust.

Thus, though users may not differ in their beliefs of the actual data collection behaviour of the app, their trust in the app still varied depending on the framing of the evidence and their perceptions of the recipient of the data, as evidenced by the cases comparing conditions with the securitizing narratives regarding Chinese government access to data with their corresponding American conditions. In most cases, the users accepted the same facts (evidenced by similar distributions of data collection assessment), but responded to the facts differently. In particular, we note that though users believed similar amounts of data were going to the US government and the Chinese government, they were more distrustful of this data flow to the Chinese government.

5.5 Effects of Personal Relevance

We used the frequency with which respondents used the app to measure their personal relevance to the application. Of the 829 respondents, 650 (78.4%) had used the app
they saw before. Of those who had not used the app, only 3 had not heard of the app they saw. Thus, less than 1% of respondents had neither used nor heard of the app.

Due to different initial trust levels, we do not have any conclusive evidence to support H6, with slightly different $p$-values when comparing users and non-users of an app and high versus low frequency users (Table 5.7).

We first analysed the data by dividing respondents into two broad categories of personal relevance: those who have used the app and those who have not. For respondents in both of these categories, there was significantly less trust after being presented with an argument. These changes were in the direction expected, with decreasing levels of trust, showing that the arguments were persuasive for both users and non-users of the app. We then compared the distributions of trust of users between the two groups after treatment to understand whether arguments were more effective for those with lower relevance to the app. There were significant differences between those who have used the app and those who have not ($p < 0.001$), with those who have used the app having more trust than those who have not used the app. Thus, though users of the app were significantly more likely to be persuaded by an argument ($p = 0.028$), the effect is not strong enough to match the distrust of non-users, and was likely due to the higher initial trust levels of those who use the app, allowing persuasion as we defined it to be more possible to occur.

Within the respondents who have used the app, we further divided them into high and low usage, with those in the high usage category using the app at least “Several times a day” (7 or higher on the Likert to numerical scale conversion) and those in the low usage category using the app at most “Once a day” (6 or lower on the Likert to numerical scale conversion). We ran the same tests as we did for comparing between those who have and have not used the app. Results can be seen in Table 5.7.

For both high and low usage groups, there were significant decreases in trust ($p < 0.001$), as expected. There were also significant differences in trust levels after
Figure 5.5: Probability for each level of trust by frequency of app usage

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Odds Ratio</th>
<th>p-val</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nationality</td>
<td>0.817</td>
<td>0.138</td>
</tr>
<tr>
<td>Language</td>
<td>0.768</td>
<td>0.043</td>
</tr>
<tr>
<td>Government Access</td>
<td>0.734</td>
<td>0.018</td>
</tr>
<tr>
<td>App Usage Frequency</td>
<td>1.26</td>
<td>&lt; 0.001</td>
</tr>
</tbody>
</table>

Table 5.8: Odds ratios and p-values for each of the three independent variables present in the argument as predictors in an ordinal regression model.

treatment between these groups. High usage users tended to have higher levels of trust than did those who used the app fairly infrequently. Despite the higher levels of initial trust, high frequency users were less likely to be convinced by an argument than low frequency ones, though this falls just above the 0.05 significance threshold. In all other cases where one group’s initial trust was higher (e.g. by app nationality, by use vs non-use of app), that group found the argument more effective, but the reverse was true for app usage frequency for users of the app. Thus, it is likely that individuals who use an app frequently have a particularly strong belief perseverance of their trust in an app. This may imply that arguments, though persuasive for both groups, were more effective for those who were infrequent users of the app than those who were high frequency users.
We were also interested in the ways in which personal relevance to the app affected how users processed arguments and so ran an ordinal logistic regression to predict trust levels post-treatment with frequency of use of the app as a fourth predictor in addition to the three independent variables. The four predictors were thus: the three independent variables in the argument (app nationality, language, government access) as indicator variables and frequency of use of the app on a scale of 0 to 10. A 0 for frequency meant the user had not used the app, while a 10 meant that the user responded that they used the app “All the time.” The results are seen in Figure 5.5 and Table 5.8. When app usage frequency was included as a predictor, the nationality of the app was no longer statistically significant ($p = 0.138$) while the tone of language used in the app just barely becomes significant at the 0.05 level (though not significant after corrections for multiple comparisons) and claims of government access to data remain significant in predicting trust ($p = 0.018$).

With each unit increase in frequency of app use (used to represent an increase of 1 level in the ordinal scale for usage frequency), users were 1.26 times as likely to find the app more trustworthy. In other words, the more often someone used an app, the more likely they were to find an app trustworthy. This effect can be seen in Figure 5.5. As shown in the graph, the likelihood of believing that an app is “Very untrustworthy” decreases almost linearly with the frequency of app use. While the likelihood of believing an app is “Somewhat untrustworthy” increases for lower levels of use, as those who would have otherwise said “Very untrustworthy” now only believed the app is “Somewhat untrustworthy.” However, at around 6 or 7 (those who use the app once or several times a day), the probability of believing the app is “Somewhat untrustworthy” decreases, and the likelihood of seeing the app as “Somewhat trustworthy” rises. Therefore, this supports the idea that those we classified as high frequency users of an app were much less affected by arguments.

Interestingly, this regression model suggests that nationality of the app does not
Table 5.9: Mean trust in an app, before and after being presented with the argument, sorted by personal relevance to the app. The “Yes” category includes all users who have used the app and the “No” category those who have not. The “High” frequency category includes those who use the app several times a day or more, and the “Low” usage category consists of those who use the app at most once a day. Lower numbers indicate lower trust. The $p$-values result from pairwise tests between those who saw TikTok (TT) and those who saw Instagram (Insta.).

5.5.1 Usage of App Moderates Effects of App Nationality

The app to which users were randomized heavily influenced their perceptions of the app both before and after reading the argument, as seen in Section 5.2.1. However, we now control for personal relevance to see if it moderates the effects of app nationality. Thus, we compared trust levels between users assigned to different apps, divided into subgroups by their personal relevance to the app. These results are seen in Table 5.9.

Initial trust was different between apps, in all cases except the group with high usage of either app. For those who infrequently used the app and for those who have not used the app, users were more distrustful of TikTok than of Instagram, consistent with other observations. Furthermore, when only looking at whether or not an individual has ever used the app, trust levels still varied between apps. It was only when separating out those who use the assigned app at least several times a day that preheld trust levels were no longer significantly different, meaning this particular subgroup of high frequency app users do not generalize to all users of the...
app. There was also no significant difference in trust between users with high usage of TikTok and Instagram after treatment \((p = 0.491)\), suggesting that high personal relevance to an app overrides the effects of the app’s nationality as a cue for trust evaluation. Arguments were similarly effective for high frequency users of either app, as the proportion of users convinced were not statistically different \((p = 0.161)\).

For the other three categories, due to the differences in initial trust, we did not find the results for effectiveness of argument particularly illuminating, as initial distributions would affect the proportion of users that could be persuaded by our definitions. Nevertheless, they were included for completeness.

The only difference in trust after treatment that was significant after corrections was when grouping all those who used an app (regardless of usage frequency) into one category. As the effectiveness of the argument was not statistically significant between apps after corrections, this result is likely due to the differences in initial trust carrying forward.

The only category for which argument effectiveness differed between apps after corrections for multiple comparisons was for those who did not use the app \((p = 0.008)\). For non-users of Instagram, arguments regarding Instagram were more persuasive to the point that distributions of post-treatment trust did not differ between apps \((p = 0.151)\). From this, we hypothesized that for non-users of apps, arguments may cause greater magnitudes of change, and so they were more easily convinced due to lack of personal relevance to the issue. This then led to the result of similarly low distributions of trust between apps after treatment when initial trust was significantly lower for TikTok.

The results that personal relevance moderates effects of app nationality are further confirmed by our ordinal regression wherein app nationality was no longer significant after accounting for frequency of app usage. These results, in combination with the regression results, suggest that not only are arguments less effective for those with high
### Table 5.10: Odds ratios and $p$-values for each predictor in an ordinal regression model

<table>
<thead>
<tr>
<th>Predictor</th>
<th>Odds Ratio</th>
<th>$p$-val</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nationality</td>
<td>0.796</td>
<td>0.098</td>
</tr>
<tr>
<td>Language</td>
<td>0.752</td>
<td>0.030</td>
</tr>
<tr>
<td>Government Access</td>
<td>0.737</td>
<td>0.020</td>
</tr>
<tr>
<td>App Usage Frequency</td>
<td>1.24</td>
<td>$&lt; 0.001$</td>
</tr>
<tr>
<td>Economic Views</td>
<td>1.12</td>
<td>0.148</td>
</tr>
<tr>
<td>Social Views</td>
<td>0.928</td>
<td>0.361</td>
</tr>
<tr>
<td>Technical background</td>
<td>2.73</td>
<td>$&lt; 0.001$</td>
</tr>
</tbody>
</table>

personal relevance to an app, but that they supersede any effects of app nationality entirely, which was otherwise the most effective of the three independent variables.

### 5.6 Demographic Effects

We also explored the effects of background variables, such as a user’s social and economic views, as well as whether they have a technical background, on how they perceived an argument. To do so, we ran an ordinal regression model using seven predictors, the three independent variables in the argument, and four variables that described the user: how often they used the app, their economic views, their social views, and whether they had a technical background (Table 5.10).

Our model predicted that users were slightly more likely to find an app untrustworthy the more economically conservative they viewed themselves to be. It also predicted that the more socially liberal they reported themselves to be, the more untrustworthy they found the app. However, neither of these predictors were statistically significant ($p = 0.149$ and $p = 0.361$ for economic and social views respectively).

Having a technical background did have a strong influence on trust overall, supporting H7a. Those who reported a technical background ($n=260$) were 2.73 times as likely to find an app more trustworthy than someone without a technical background ($n=569$, $p < 0.001$). Similarly, through pairwise comparisons between the groups, trust was found to be significantly higher for those with a technical background than
those without, both before \( (p = 0.001) \) and after \( (p < 0.001) \) treatment. We suspect this may be due to the arguments being less alarming for those who are more familiar with the behaviour and data collection practices of apps, and thus being less alarmed by arguments detailing activity by either TikTok or Instagram that are not wildly outside the usual practices of most applications. There may also be a familiarity bias, as prior work has found that those with more familiar with the app ecosystem tended to have higher levels of trust and less perceived risk [31].

However, there was no support for H7b as trust still differed significantly between apps even between those who had a technical background, with lower overall trust for TikTok relative to Instagram before \( (p < 0.001) \) and after treatment \( (p = 0.001) \). Therefore, despite overall higher levels of trust for the two apps in general, those with technical backgrounds still tended to trust TikTok less.
Chapter 6

Discussion

Given the ongoing securitization of technology, and particularly of Chinese technology, in current US political discourse, we aimed to understand the effects of such argumentation on the general populace. There has been much work done on the way technology, and in particular social media, has influenced politics—such as the rise of increased partisan polarization facilitated by media bubbles and the spread of disinformation and misinformation. However, this influence does not flow only one way, as politics also changes the way in which the public perceives technology. Understanding that public opinion can influence public policy [11], it is important to understand the effects of securitizing an application so prevalent in the daily lives of citizens in an era of increased distrust.

Due to the random assignment of participants to conditions, we can claim causality of the independent variables (app nationality, language, claims of government access to data) used in constructing the arguments and their persuasiveness. Our results showed that each of our three variables (either alone or in combination) reduced user trust in a mobile application and further suggested that certain types of securitizing moves are effective. We also note that the frequency of use for an application moderates the effects of nationality of an app, with arguments being similarly effective
for high-frequency users of either app, while non-users have similarly high levels of distrust after treatment.

6.1 Nationality

Nationality of the app was one of our three independent variables and one of the main elements of the securitizing narrative surrounding TikTok. We explored it to understand whether negative public opinion of TikTok was influenced by the securitizing moves targeting it, or simply by general public wariness of technology companies and their data collection practices. As the vast majority of participants (over 90%) were aware of the nationality of the app they saw, we believe the nationality of the app played a role in the way users assessed their trust and beliefs. Our belief that nationality was the factor influencing differences between the TikTok and Instagram cases cannot be explained using only the difference in their reputation, even though reputation is a factor known to have effects on trust [48, 36]. This is in part due to the fact that reputation as measured in these studies often use the popularity of the app as a proxy, but both apps we investigated are similarly popular, having been consistently in the Top 10 free apps on the US App store since May 2020 [4]. As most studies that vary reputation as an independent variable do so by varying reported popularity (whether by rankings, user reviews, or number of downloads), they thus are unable to fully account for other cues (such as media attention) that may play into the construct of “reputation” [13, 60, 48, 52]. Thus, the differences in trust in the app did not come from their reputation as commonly constructed in prior work, or at least not from reputation alone. Therefore, although reputation of the apps likely played a role in user perceptions, we specifically isolated nationality and its links to the existing securitizing narrative in our investigations.
6.1.1 Differences in Initial Trust Between TikTok and Instagram

In order to measure within-unit changes, we asked participants both before and after treatment to evaluate their trust in the app they saw. Thus, app nationality was the only independent variable participants were exposed to before treatment, and the only one with differences in initial trust. Since news about TikTok was covered extensively by media, particularly in summer 2020 during the period around Trump’s proposed TikTok ban, it stands to reason that many respondents would have had prior exposure to information about TikTok. Indeed, although singular news stories rarely are enough to change individuals’ political opinions regarding candidates and officials, the repeated exposure through media to negative information about an issue can reduce support [59, 39]. Thus, as coverage about the proposed ban often included Trump’s justification of national security concerns and vilification of the app and its parent company, repeated exposure to such information would have likely shaped the preheld views of many users. Nevertheless, it is also worth noting that the media attention around TikTok and the securitization arguments surrounding it were most prevalent during summer 2020. However, this study was run in spring 2021, yet there still existed less trust of TikTok than of Instagram, even after more than half a year since the original announcement of the TikTok ban by the Trump administration. This suggests that these arguments have staying power, and continued to shape public perceptions of mobile apps, and in particular, Chinese apps, even after the height of the media attention.

Due to this difference in preheld conceptions regarding the apps, we controlled for initial trust levels. Namely, we compared the persuasiveness of arguments regarding TikTok against those regarding Instagram for all users who were initially neutral about either app, and similarly for those who felt it was “Somewhat trustworthy” and then “Very trustworthy.” We found that when users with the same initial trust levels
of an app were treated as one group, they found arguments equally convincing for TikTok and Instagram. This implies that the group that initially distrusted TikTok was a significantly different subpopulation.

We have two hypotheses about the reason for the significantly greater proportion of users that had lower initial trust of TikTok. The first is that due to the constant negative media coverage of TikTok, users internalized these arguments simply due to exposure to these claims and there was little absorption or conscious consideration of the securitizing moves that happened around these arguments. Had the news coverage been around an American company (say, Facebook), this population would have had similarly low trust. However, as there was no large scandal surrounding Instagram, initial trust differed between the two apps. If this is the case, then securitizing moves merely linking TikTok with China would not be more persuasive, and this also explains our result that the arguments for both apps were equally effective when controlling for initial trust.

The second hypothesis is that securitization arguments were broadly successful, and it was the explicit linking of TikTok to China that made this population change their mind and gave the arguments staying power. Indeed, news and online discourse surrounding the proposed TikTok ban often included mentions of TikTok being owned by a Chinese company. Therefore, a securitizing factor played into the acceptance of these arguments and lasting attitude change of increased distrust towards TikTok. Using ELM to understand the lasting effects of these arguments, it would mean that those who continued to hold lower trust of TikTok even months after the height of the media attention carefully considered (i.e. elaborated upon) the securitizing arguments given as justification, and found them to be convincing [62]. Under this hypothesis, the remaining population would thus have either not have been convinced by the arguments they saw in 2020 regarding TikTok, or did not form lasting attitudinal changes. Thus, this may explain why arguments were equally effective for both apps.
conditioned on prior trust—the population that did not already distrust TikTok held no strong anti-China/anti-Chinese technology feelings, and thus nationality of app was not a big concern for this population. However, this group is then different from the general American population, as those who would have been convinced by the securitizing arguments already not trustful of TikTok.

### 6.1.2 Overall Trust Levels

We further found significant differences in trust levels after treatment between TikTok and Instagram. Due to the lack of clarity regarding the higher distrust of TikTok than of Instagram because of differing initial trust levels, we note that this pairwise analysis of overall trust levels post-treatment could be taken as a snapshot of broader American views given that securitizing arguments have already been made regarding TikTok. Namely, in a situation where there were claims about a Chinese app as a threat, there would overall lower trust of that app. However, we cannot say with certainty that the outcome would have not been the same for an American app. Indeed, Facebook, another social media platform that has similarly been riddled with scandals (Cambridge Analytica and the $5 billion settlement in 2019 with the FTC) inspired similar levels of distrust among Americans (42.6%) as did TikTok (43%) [20, 24]. Therefore, it may have been media coverage that lead to this distrust rather than securitizing claims. However, we also note that the proportion of Americans that found Facebook trustworthy (37.8%) was significantly higher than for TikTok (28.1%) [20], which suggests there may still be differences between the US public’s views of American and non-American companies facing similar claims regarding data collection and infringement of privacy.

It is also worth noting that the vast majority of respondents were aware that TikTok was owned by a Chinese company. We speculate that it was the negative media attention and the linking of TikTok with China that made users aware that
it was a Chinese app, as Google searches including the keywords of “TikTok” and “China” or “Chinese” spiked around summer 2020. Nevertheless, even if distrust of TikTok was due to negative media exposure—rather than seeing TikTok as a threat—though there may not have been specific articulated ties within users’ minds about Chinese apps being less trustworthy, then these connections between TikTok, untrustworthiness, and China are still being made, propagated, and retained. This lack of trust may further build on existing prejudices of China and Chinese products as inherently untrustworthy, feeding into an ongoing securitization narrative about China in the US. The consistently lower levels of trust for TikTok, both before and after treatment, indicate a strong correlation between the nationality of an app and distrust in the app. However, we cannot claim causation as this lack of trust in TikTok may not have been specifically influenced by the securitization arguments but rather by media exposure. Therefore, the link between trust, media coverage, and securitizing narratives warrants further study.

6.2 Government Access to Data

We also explored the effects of claims that a government had access to user data collected by the app. Thus, certain arguments included an explicit statement that the data was being shared with the government of the respective app. This allowed us to understand whether the claims about TikTok were convincing because of the securitizing move of linking this data collection specifically with the Chinese government, or whether any government’s access to data would have been similarly alarming.

Overall, without controlling for app, we found that arguments that stated governments had access to data were more effective than those without, resulting in lowered overall trust and higher probabilities of finding the app untrustworthy. Therefore, the idea of any government accessing user data was alarming. We further divided
our analysis by application, looking at arguments about Instagram, which claimed the US government had access to user data, and then at TikTok, whose arguments claimed it was the Chinese government that had access to this same data.

We found that for Instagram, arguments that stated the US government may have access to user data were significantly more effective than ones without. The Pew Research Center has found that Americans are generally more concerned about companies (79%) collecting their data than the government (64%) [6], while we found that trust was actually more likely to decrease when claims that the US government to data were present. However, this does not contradict the Pew Research Center results, as they asked about data collection generally whereas we explored it in the context of a specific application and corporate sharing of data with the government. Thus, the reduced trust in our case may have been due to an unexpected actor (the US government) also having access to data, when such data would generally be assumed to only go to the company.

Arguments about TikTok that included an extra explicit statement that the data collected by TikTok may be shared with the Chinese government were also seen to be significantly more effective than arguments without that claim, though resulting trust distributions were not significantly different (despite a lower median trust of 1). This lack of significance in overall trust levels despite differences in effectiveness may be simply due to the underlying distribution of our data. It may also be due to the fact that some users that would have greatly decreased their trust in TikTok even without the argument explicitly claiming it was related to the Chinese government. This could be that given the securitizing narrative propagated around TikTok, any associations with Chinese companies would be already being linked to data being shared with the Chinese government, and thus was not an extra factor for certain users when evaluating trust.

It would thus appear that the effect was much more pronounced for Instagram
(66.7% persuaded) than TikTok (53.7% persuaded). We hypothesize this may be due to users never having been previously exposed to arguments claiming the US government had access to data from Instagram, whereas the news surrounding TikTok brought to the forefront the claims that the Chinese government was in league with ByteDance and collected American data. If this was indeed the reason for the lack of difference in TikTok’s distribution of trust, that implies that there may already exist in users’ minds an implied link between TikTok and Chinese government having access to that data. Thus, without needing to explicitly state that a Chinese company was connected with the Chinese government, users would already make that connection without prompting.

6.3 Securitization

To more clearly understand the effects of alleged government access to data, we compared across conditions that only varied in the app’s nationality. We specifically compared between Instagram and TikTok in the conditions where the government was said to have access to user data. Trust levels after treatment were all significantly different, with less trust for TikTok and a higher likelihood to find TikTok untrustworthy than Instagram. The lower levels of trust for TikTok may also have been due to lower initial trust in TikTok. However, the amount of data users assessed the app to be collecting was the same between apps in all conditions of interest. Therefore, this suggests that it was not simply the amount of data that was being collected that was alarming to users, but rather the fact that this data was claimed to be going to the Chinese government rather than the US government. From this, we believe that the lack of trust in TikTok arose not solely due to the claims of data collection, but also its interaction with beliefs that a foreign government had access to user data.
From the discrepancy between the data collection perceptions being the same but trust being lower, we do have reasonable cause to believe that securitizing moves stating user data was shared with the Chinese government have a negative impact on trust beyond additive impacts of concerns regarding data collection and the government access. It would mean that similar data collection and sharing behaviour for an American and a Chinese app would be viewed differently. Thus, even though two-thirds of Americans are concerned about how the US government uses collected data [6], and though users would still be wary of an American app, they would still be more suspicious of a Chinese app with the same behaviour because it was the Chinese government rather than the American one accessing their data.

6.4 Language

Another independent variable we explored was the language and tone with which the argument was presented. This variable allowed us to better understand the technification aspect in cyber securitization, in that when relatively more “technical” issues are securitized (e.g. technical details of data collection), experts are able to frame and shape the discussion as the general population feels less qualified to parse the details. Thus, half the participants were presented with arguments written in relatively neutral language, while the other half with arguments using alarmist language framing the app’s data collection behaviour as out of the norm and extremely suspicious. The data is somewhat unclear on the effectiveness of this variable, with $p$-values often lying just above or below the threshold of statistical significance after corrections. Trust was indeed lower after treatment for conditions with alarmist language, though these arguments were not shown to be more persuasive when looking at overall proportion of users convinced. In other words, average levels of trust dropped more under alarmist conditions, but the fraction of people persuaded was not significantly
different between arguments using neutral or alarmist language. Thus, there is some preliminary evidence to suggest that alarmist language has an effect on trust if users feel less able to evaluate the technical details of the argument on its own merits. This may also give one preliminary explanation for the persuasiveness and virality of the Reddit post, which heavily used technical terms and acronyms, and framed the information given in an alarming tone, positioning TikTok’s data collection as extremely suspicious [80].

We hypothesize that perhaps alarmist language is not necessarily more persuasive, but rather causes a bigger change in trust levels, or perhaps more lasting change for those who find the argument convincing. Future work could thus test for the durability of changes in trust levels. We also believe the technification aspect of cyber securitization and on the presentation of claims and arguments regarding apps and technology warrants further investigation. In particular, language could be varied even more dramatically, with increased use of specialized, technical vocabulary making it difficult for lay users to parse, and thus possibly rely more on contextual clues to understand the argument.

6.5 Personal Relevance to App

We also found that although users were generally persuaded by arguments, the personal relevance a user had to an app, as measured through their usage of the app, affected the effectiveness of arguments. Users with higher usage frequency of the app were less likely to be persuaded by the argument, and more likely to find the app trustworthy. From this, we can extrapolate that apps with more active users would be less likely to be affected by claims of their untrustworthiness due to their higher relevance to the population.

Two user populations of particular interest were the high frequency users of an app
and the non-users of an app. For both of these groups, the presence of securitizing elements in arguments did not appear to be persuasive, though the hypothesized reasons for this lack of effectiveness differ for each population.

Between high frequency users of either app, there were no differences in trust levels either before or after treatment. The argument was also similarly effective for this group, whether the participant saw TikTok or Instagram, and thus arguments involving securitizing moves were not better at decreasing trust for those who use the app at least several times a day. Unlike all other populations, there was no lower initial trust in TikTok than Instagram, despite these users likely having been exposed to the same arguments through news media. This further reveals that for those with extremely high relevance, neither negative news coverage nor securitizing arguments regarding an app were effective. These results parallel the findings that those who are well-informed about politics tend to be most difficult to persuade through information from media [39, 59]. Although personal relevance is not directly parallel to political knowledge, it stands to reason that higher levels of usage and higher personal relevance indicate an existing connection with and knowledge of the app and its practices, and the fact of continued usage means that the arguments made against TikTok were broadly unsuccessful in convincing this population to discontinue their use.

Another possibility for the lack of difference between apps for high-relevance users—given that this study took place after the announcement of, and media attention surrounding, the TikTok ban—is that there were individuals who were no longer high-frequency users after the media coverage about TikTok. This ties into the second hypothesis from Section 6.1.1 in that those who would have been persuaded by the securitizing moves were already convinced before the study, and thus discontinued their usage of TikTok. Those that remained high-frequency users of TikTok consisted of individuals that did not and would not find securitizing arguments persuasive and thus did not differ from high-frequency users of Instagram.
The non-users of an app, though they had differing levels of trust between apps before treatment, did not have different trust distributions after. This suggests that it may not be the securitizing elements present in the argument, but rather the mere act of presenting any information stating that an app such individuals had little relevance to that was effective. We hypothesize that due to low personal relevance, when presented with an argument, users that feel no particular attachment to the app would be convinced without much difficulty, and thus have large decreases in trust. Therefore, due to the already lower trust of TikTok, users may have already had some suspicion of the app due to prior media exposure, but the effect was much more pronounced for Instagram, where attitudes were generally more trusting. Therefore, for people with “no skin in the game” so to speak, regardless of prior impressions of the app, if explicitly told that an app is untrustworthy or behaving in dubious ways regarding data collection, trust would immediately decrease to some lower bound, whether that app was American or not. Thus, we believe for those who did not use the app, it is not securitizing arguments that are effective, but simply negative media coverage and exposure to arguments about the dangers of the app.

Within the high usage and non-usage populations, trust distributions were similar between apps after treatment, and seem to show that securitization arguments are not more persuasive when made to these groups, but for different reasons. For the high relevance users, due to existing connections to the app, they may evaluate the arguments more carefully [62], hold preformed positive opinions, and thus not change their mind as much due to securitizing moves. As for the non-users, arguments regarding suspicious data collection were always extremely convincing, decreasing trust to the lowest or nearly the lowest possible, regardless of app. However, this required that these users be presented with these arguments and negative portrayals of the application. Therefore, because it was TikTok that had this negative media coverage surrounding it, there was lower initial trust of TikTok. Nevertheless, had
the media coverage been for another app (even an American one), then we suspect we would have seen similar low levels of trust for non-users.

These findings around the effects of personal relevance as mitigating securitizing effects are particularly interesting when comparing TikTok and Huawei. As Huawei was successfully put on the Entity List whereas no actual ban of TikTok could be enforced, Huawei’s lack of relevance to the general US population may have played a part. Since there were likely few Americans with high personal relevance to Huawei [12], the securitizing moves and negative media coverage would have been effective in reducing trust and confidence in Huawei. Furthermore, as non-users were not particularly sensitive to securitizing arguments but generally less trustful, the repeated media exposure to Huawei as a threat would have been persuasive, perhaps even if it had not been deemed a Chinese threat. Nevertheless, the securitizing moves being made around Huawei was necessary in justifying government action, which was the end goal of undertaking any securitizing move in the first place [85, 9]. Thus, because the government wanted to take action, creating a securitizing narrative was necessary, and furthermore built a foundation and precedent for further similar moves against other Chinese technology companies such as TikTok.

6.6 Technical Background

We found that those with a technical background were more likely to find an app trustworthy, which is in line with previous work that found those with more familiarity with the Internet or the app ecosystem tended to have lower perceptions of risk [87, 31]. We theorized that perhaps those with technical backgrounds would be less convinced by arguments regarding TikTok (whether in initial trust or trust after treatment) due to the ability to more accurately parse technical claims and not be as swayed by contextual cues such as “technified” language. However, we did not find
evidence to support this hypothesis, as trust levels for those with a technical background still differed between the two apps. Nevertheless, considering ELM theories of persuasion, this may also be due to relatively low relevance to the topic (for example, if those with a technical background did not often use the app) and thus still being persuaded by peripheral cues such as media exposure to TikTok’s “malicious practices” or not deeply evaluating the arguments despite having the ability to do so. Furthermore, prior work has also suggested that though individuals with a general technical background may feel generally higher comfort and familiarity with technical terms, they still may not hold completely accurate perceptions of said terms [77]. This aligns with our results of higher trust levels of the apps overall, while still seeing a discrepancy in trust between TikTok and Instagram. Therefore, we cannot completely discount the idea that those with a technical background are less persuaded by securitizing arguments, although this warrants further exploration.

6.7 Data Collection

One of the main the securitizing moves regarding TikTok was that not only was data collected by the app, but that this data was being shared with the Chinese government. Thus, in our study, each arguments presented that the same amount and types of data were collected, but to varying actors. This allowed us to disentangle whether it was the data collection itself that was viewed as problematic, or if there were other factors causing distrust. We asked participants how much data they believed the app was collecting both before and after treatment to see if the same basic information was interpreted differently in arguments with different framing and contexts.

Interestingly, users generally believed TikTok collected more data than Instagram, both before and after treatment, even though users were presented with the same set of facts for both apps. This could be due to media exposure to news about TikTok
collecting and giving data to the Chinese government, and thus TikTok being already associated with high data collection. Thus, the nationality of an app affected the ways in which users understood arguments when the same information was being presented. However, the same amount of data was perceived to be collected for TikTok and Instagram in the specific cases where their respective governments were said to have access to that data. The implications of this were previously explored in Section 6.3.

Across the variables of language and government data access, users did not vary in the amount of data they believed was collected overall, even though trust distributions differed. This implies that although individuals are generally concerned about data collection and feel little control over their personal data [45, 6], the amount of trust was also due to which actors users believed had access to their data. From the results showing higher distrust in the government access conditions though data collection assessment remained broadly similar, we believe that users were generally more suspicious of government access to data due to the explicit mention of the US government as a recipient of the data from a social media app, when users generally only expected the company to have this data, agreeing with understandings of privacy as contextual integrity [55].

However, even when individuals believed an app’s behaviour was the same, their trust in the app can still vary depending on other factors. Trust is influenced by context and perceived risk, so concerns over data collection and use may be more salient if the situation feels like more of a threat to the individual. Indeed, as trust can be conceived of “as the willingness to be vulnerable under conditions of risk and interdependence” [69], yet if the risks of data collect are seen as too high and the trustor does not want to be vulnerable to the actor (whether it be any government or specifically the Chinese government), then we see lower levels of trust. Therefore, concerns over an app and trust in an app are not due to its data collection practices
alone, but also are influenced by which actors are in possession of that data, and the attitude that the user holds towards these actors.

6.8 Political Implications

Due to the timing of the study (post-TikTok ban), we cannot say with confidence that our three independent variables alone were the sole causal factors in differences of overall trust after treatment in circumstances where there were differences in initial trust distributions. However, we did see marked differences between TikTok and Instagram apps and the attitudes of users towards these apps overall. A possible future direction would be to vary the same variables, but with a hypothetical app, so that there were no prior manipulations of, nor differences in, trust. We also found a subpopulation—high frequency users of an app—for whom securitizing elements were not seen to be more persuasive. Furthermore, it appears that although data sharing with the government is generally alarming to users, the compounding factor of it being shared with a foreign government is particularly alarming. Thus, it is not only data collection, but also perceptions of the recipient of the data that plays into a user’s evaluation of trust. We now tie these findings back to the broad securitizing narratives that surrounded TikTok near the end of the Trump administration.

One part of the securitizing claims were predicated on data collection being alarming, with Executive Order 13942 stating that, “This data collection threatens to allow the Chinese Communist Party access to Americans’ personal and proprietary information” [83]. Our results revealed that users thought the same amount of data was collected by TikTok and Instagram in the specific cases where the data was said to be going to either the US or Chinese government, but were less trustful in the conditions with claims that this data was going to the Chinese government. These results suggest that the explicit link made between data collection by TikTok and this in-
formation going to the Chinese government was more alarming than if it had been to the American government, and so in this sense, the securitizing move was more persuasive to the American population.

The other broad stroke of the securitizing moves around TikTok were the ties to China itself, as EO 13942 states that “the spread in the United States of mobile applications developed and owned by companies in the People’s Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States” and does not distinguish between different types of Chinese apps nor specify what exactly in their behaviour constitutes the threat [83]. Instead, this broadly makes the implication that TikTok is inherently untrustworthy simply because it is Chinese. Though overall trust was lower for TikTok, our results did not give any conclusive evidence that this lower trust was due to securitizing moves against TikTok rather than the media exposure overall. Thus, though our results suggest that there is a correlation between knowing an app is Chinese and having less trust in an app, we cannot state that the knowledge of an app being Chinese was the cause of this.

Past work has further found that the tech company Americans trusted second-least was Facebook, just after TikTok [20]. However, there were never securitizing arguments made regarding Facebook, but just negative press coverage, so it seems that repeated exposure through media to arguments of Facebook’s malfeasance caused broad distrust in Facebook. Therefore, the lower initial trust of TikTok cannot be attributed to securitization alone. Even if the lack of trust was due to repeated media exposure, it would appear that this suspicion (regardless of origin of app) is often concentrated towards specific apps and companies that were in the spotlight. Indeed, other Chinese-owned apps, particularly game apps, have enjoyed and continue to enjoy widespread success with US audiences, in particular gaming apps such as PUBG and Genshin Impact. Thus, negative public opinion may be formed due to
the negative attention rather than the securitization of the technology. Nevertheless, the securitizing moves that originated this media attention are still important from a political standpoint, as they are necessary to allow more government latitude in actions declared necessary against what was framed as an existential threat, even if it is not the existential threat argument that made the public not trust it.

Overall, it appears that there is significantly less trust of TikTok than of Instagram, with the most effective predictor of trust being the nationality of the app, when not accounting for personal relevance. The use of securitizing moves to reduce trust in Chinese technology has been seen to be broadly persuasive, whether through news media or through the securitizing arguments themselves, resulting in overall markedly lower levels of trust. This aligns with other moves, including the previously successful securitization of Huawei as a threat the US critical infrastructure, and the current ongoing positioning of China as a threat in the domain of Artificial Intelligence [66]. The propagation of, and persuasiveness of, such arguments is concerning. If the public continues to associate not merely a particular app or company with national security concerns, but rather any technology produced by a Chinese entity, then this would allow continued policy targeting foreign technology merely on the basis of its foreign origin.
Chapter 7

Limitations and Future Directions

Due to the nature of our study, we reflect here upon some limitations to consider when interpreting the results and conclusions from our data. We explore these limitations in context below, and where relevant, suggest some future avenues of research.

7.1 Survey Design

7.1.1 Attention Check

Due to the nature of Amazon MTurk, we could not be certain that all respondents carefully read and processed the paragraph containing arguments about the app. Thus, we both collected data about how much time respondents spent on the page with the argument and included a question with a textbox that asked respondents what they believed the nationality of the app to be. The open-ended textbox question also functioned as an attention check. We rejected responses that were nonsensical, irrelevant to the question asked, or answered with one of the statements we explicitly stated would be rejected (i.e. “None” or “I don’t know”). For responses that were borderline acceptable, we cross-referenced the amount of time spent on the page containing the argument and rejected responses that spent less than 2 seconds on the
Nevertheless, this still does not ensure that all users fully read the argument—though this variation may be analogous to a real-world scenario, as not all those who encounter new information fully take time to consider such information but may rather form opinions through repeated exposure to certain concepts [39].

As we rejected responses that answered “I don’t know” when we asked respondents for their best guess as to the nationality of the app, this may have led to us filtering out a population that was significantly different that our resulting sample population—those who genuinely did not know the nationality of the app they saw. However, as our question explicitly asked respondents to put in their best guess, we still likely received responses from users who did not know the nationality of the app but rather guessed the answer (correctly or incorrectly). There is indeed value in examining those who are unaware of the nationality of Instagram or TikTok further as a separate population, though due to the prevalence of TikTok in the news and the possible difficulty of distinguishing answers of “I don’t know” that were genuine and those that were automated or from those who did not pay attention to the survey, we did not consider this population in our analysis.

7.1.2 Language Variable

Our second independent variable—whether the argument used alarmist or relatively neutral language—manipulates a few factors of interest in the same variable in that it ties into both alarmism and technification. Both conditions included technical language, though the alarmist conditions specifically argue that the data collection undertaken by the app is dangerous and alarming. This thus ties into the idea of technification insofar as the argument, leaning on technical specifics and assumptions of the source’s “expertise,” claims these actions are out of the norm and threatening. However, this is coupled with the use of alarming language, heightening the sense of
threat and alarm and possibly adding to the argument’s persuasiveness. With technification alone, relatively neutral language may also have similar effects of decreasing trust, even without using arguments presented in an alarming tone. Therefore, it is likely that both alarmism and technification played a role in the effects of the language variable and thus warrants further study, possibly as separate variables.

7.1.3 Personal Relevance

The division of personal relevance into by high and low usage on those who used the app “Several times a day” or more often and those who used it less may have caused some loss of nuances between other possible categorizations of personal relevance. For example, those who rarely used the app and those who used the app once a day are both grouped into the low relevance category, despite distinctions likely existing between these subpopulations. It is possible that we could have classified those who used the app “Once a day” as high usage users. However, as Instagram and TikTok are social media apps, it is reasonable to consider only those who used the app more than once a day as the high usage population due to social media necessitating relatively more engagement with these apps to be constantly up-to-date on these platforms.

As we examine specific applications in this study, it is not clear whether these results generalize to all high-frequency users of all applications. Indeed, to the best of our knowledge, no other work has specifically measured the relation between trust and usage of specific services and applications. Most of the work in this space focus on more general traits of the user, such as overall Internet or app usage, or technical expertise rather than specific connection to the application [31, 87, 33]. This is in part due to the tendency to conduct user studies for hypothetical apps and websites rather than established ones to reduce prior bias. However, as we investigate the actual political context surrounding TikTok, we were able to measure relevance through usage of the specified apps, allowing for more nuanced study. This warrants further
inquiry, as it may not necessarily be the case that higher frequency of app usage overall translates to higher trust for all mobile applications, but rather only for the specific apps (or types of apps) the user is exposed to.

7.2 Data Analysis

7.2.1 Likert-type Variables

Trust and perceptions of data collection were measured in through Likert scales, which were converted into numerical factors for the purposes of our analysis. However, as Likert-type variables are ordinal data, they do not map entirely accurately to numbers. For example, the difference between finding an application “Very trustworthy” and “Somewhat trustworthy” may not be the same as the difference between finding an application “Somewhat trustworthy” and “Neither trustworthy nor untrustworthy,” though both have a difference of 1 when converted to a numerical scale. However, as our signed-rank tests examined the presence of change in trust rather than the magnitude of said change, this effect is mitigated. The Mann-Whitney-Wilcoxon tests, which tested whether the distribution of trust levels between two groups differ, also made no claims about the magnitude of the differences in between the groups but rather that they do indeed differ, and we used data such as medians and means to interpret the direction of this difference.

7.2.2 Evaluating and Comparing Persuasiveness of Arguments

As explicated in our Methodology (Section 4), we chose to define an argument as persuasive if it significantly decreased the trust of a significant proportion of users who read said argument. However, it did not allow for measurement of the magnitude of change, the difficulties and intricacies of which were addressed in Subsection 7.2.1. Regardless, general trends in changes such as a decrease in trust could be inferred
through the data by looking at means and medians, and the signed-rank test was used to confirm there was a significant shift in trust in one direction (increase or decrease) and that such trends were not due to chance.

Furthermore, we only considered those who shifted down certain broad categories in trust (ie from trusting the app to being neutral or to distrusting the app, or from neutrality to distrust) as persuaded. Thus, we did not consider those who believed the app was “Somewhat untrustworthy” before treatment and “Very untrustworthy” after or those who considered the app “Very trustworthy” before treatment and “Somewhat trustworthy” after as persuaded, as they still held broadly the same views. Nevertheless, we note that such changes, which do represent a decrease in trust, are still meaningful, and hope that the statement of means and medians for all groups illuminate these nuances.

We further evaluated the persuasiveness arguments pairwise in comparison with another argument. In other words, we defined an argument to be more persuasive than another if more users who read said argument were persuaded by it, as determined through Fisher’s exact tests. However, due to our definition of persuasiveness, it posed a difficulty when measuring users who initially already distrusted an app in that users who already distrusted an app could not be persuaded by the argument, as their trust was already in the lowest category. Thus, this posed a problem for comparisons of effectiveness when the initial distributions of trust were different (i.e. in the case of app nationality). In such cases, we explored our data further to understand the underlying reasons. Furthermore, we also looked at the distribution of results of trust after treatment through Mann-Whitney-Wilcoxon tests, and in particular those who did not initially trust the app, in order to account for those who had preheld negative feelings regarding the app, as this population appears to also be worthy of analysis.
7.2.3 Ordinal Logistic Regression

Ordinal logistic regressions assume proportional odds, in other words, that the relationship between each pair of categories is the same. For example, it assumes that the coefficients for the relationship between “Very untrustworthy” responses against all responses that were “Somewhat untrustworthy” or higher is the same as that for “Neither trustworthy nor untrustworthy” against all responses with higher trust [81]. Thus, there is only one set of coefficients for each predictor variable. This is a known feature of ordinal logistic regressions, and thus in our wording of the odds ratio, we have attempted to make it clear that the odds ratio does not explain specific trust boundaries, but rather overall likelihood of one population have a higher or lower trust than another.

Furthermore, in our ordinal regression, we chose to code certain predictors that were ordinal as continuous. These were frequency of app usage, as well as the self-reporting of social and political views. Given that we were using ordinal regressions, we had the choice to code these as categorical variables or continuous ones. Thus, we chose to preserve the ordering of these variables (i.e. treat them as continuous) rather than hold strictly true to the fact that each level within these variables may have different spacing.

7.3 Trust

The interpretation of trust varies from individual to individual, and a multitude of factors influence what we here construe in the single dependent variable of “trust” [10]. There were certainly nuances that were lost in measuring persuasiveness of the argument solely by self-reported trust. However, we did supplement the work by also asking about the amount of data the user believed was collected by the app, a relatively more objective measure. All conditions explicitly mention data collection
by the application as the cause for concern, and thus make claims regarding data collection rather than trust. We further made a distinction about the persuasiveness of the argument (measured using trust, and thus ties into the perceived risk and threat from the applications) and the way users believed the app was actually behaving (measured through data collection assessment). The parallel collection of user trust and user data collection assessment allowed for the understanding of the effects of the treatment both on a relatively more subjective level that varied by individual as measured through trust, and one that otherwise should be consistent across individuals measured through perception of data collection (across all conditions, the information presented regarding what data is collected remains roughly constant).

As this thesis aimed to understand the effects of elements present in securitizing narratives, we must recognize that measuring trust (or lack thereof) in an entity is weaker than measuring perceptions of it as an existential threat. However, we note the goal was not to understand whether TikTok was securitized, but rather the effects of the securitizing narrative surrounding it. Thus, we believe trust can be used as a proxy for understanding the overall impact of such narratives. Furthermore, securitizing actors make securitizing moves for the purpose of enabling extraordinary government action against the alleged existential threat [9]. Therefore, it is not necessary for the entire population to buy into the securitizing argument and believe in the threat, but rather enough so that any moves made against the securitized actor is legitimized. Thus, if working under such a framework of understanding securitization theory, decreased trust resulting from securitizing arguments does advance the ultimate goals of the securitizing actor in that it provides increased latitude of action due to the decreased probability of public opinion and other pushback.
7.4 Generalizability of Results

Although we can, to a degree, claim causality due to the random nature of assignment to conditions, we hesitate to claim generalizability of our results. Firstly, although results the Amazon MTurk worker population tend to generalize well [63], there is nonetheless no true random sampling from the target population (all US adults). Furthermore, though political discourse around technology and in particular, claims about Chinese technology being a threat have appeared internationally [53], these findings may not necessarily be generalizable to a non-US population. This is in part because, similar to the US framing of Huawei [12], the targeting of TikTok itself, rather than its behaviours, as a threat has been largely localised the the US.

Furthermore, we cannot be certain that our results may generalize to all Chinese apps rather than all apps that received negative media attention. The difference in initial trust between apps suggests that users already held different preconceived notions about each app, but we could not be sure whether the lower trust for TikTok was due to the securitizing arguments surrounding the app being successful or simply due to the constant media attention. Even if it was specifically the securitizing moves being made that were successful in increasing Americans’ distrust, we are still uncertain if these effects would generalize to Chinese apps beyond TikTok. This is in part due to the rather unique positioning and focus on TikTok in the American media around the ban. Indeed, a similar ban on WeChat was announced on the same day as that of TikTok [83, 84], yet has received far less media coverage. As the apps we studied (TikTok and Instagram) were specifically chosen due to their popularity and high saliency, we do not make claims about generalizability to other Chinese apps, nor to non-social media apps.

Future work could run a similar experiment using a hypothetical app so that users would not have prior conceptions of either the trustworthiness or untrustworthiness of the app, except perhaps due to users’ personal feelings regarding apps in general. Dif-
ferences between trust levels in apps after treatment could thus be attributed directly to the effects of securitizing arguments rather than possible prior media exposure regarding the entities of interest.
Chapter 8

Conclusion

In this thesis, we investigated the persuasiveness of elements used in securitizing narratives on general user perceptions of the related mobile app, in this case, TikTok. Given the prevalence of negative political discourse surrounding Chinese companies and technology—such as Huawei and TikTok—in recent years, we felt it was critical to understand the effects of these arguments on public opinion. Therefore, we identified certain elements of interest in the securitizing moves and explored their persuasiveness in arguments about allegedly concerning data collection practices of mobile apps.

The three variables we investigated were nationality of the app, the tone and language used in presenting the argument, and the presence or absence of specific claims that a government was accessing user data. App nationality and its interaction with government data access were elements that enabled the securitizing moves surrounding TikTok from the US government, and the language use possibly heightened alarm, making the data collection seem more concerning. We explored whether there were differences in the effects of each of these variables. Given our focus on securitization, we also looked more closely at claims of government access to data, and whether persuasiveness and distrust varied depending on with which government user data was said to be shared. The different outcomes of proposed government regulation
regarding Huawei and TikTok, with securitizing moves having more tangible results in the case of Huawei (i.e. its addition to the Entity List), also led us to investigate background factors, such as the relevance of the securitized entity to the individual, on persuasiveness of arguments.

From comparisons of user trust levels before and after treatment, directly stating that a certain app had concerning data collection practices always decreased trust, regardless of which variables (or combinations thereof) were present. We further found that user trust results not solely from the awareness of data collection, but also depended upon the recipient of that data. We moreover identify certain specific recipients of concern for users, finding evidence to suggest that arguments linked to securitized actors are indeed more effective, in that data transmission to the Chinese government was more alarming than the same activity to the US government. In fact, although users believed that similar amounts of data were collected by TikTok as by Instagram after being told their respective governments had access to data, the differences in trust levels between these conditions was illuminating. This suggests that the specific securitizing move of linking an actor not only with the Chinese government, but also explicitly stating that user data was being transmitted by this actor to the Chinese government, is more persuasive in reducing user trust. Given that the individual has been moved to be a referent object in cyber securitization and data security moved into the realm of national security, it makes sense that this type of securitizing argument was effective. We further saw strong correlation between an app being Chinese and lower levels of trust in said app.

These findings are particularly important in the current era of the COVID-19 pandemic. The antipathy towards TikTok as a Chinese company may have been amplified by the rising anti-Asian and anti-China sentiments that rose during the pandemic. Indeed, Huawei never became a public issue in the way that TikTok did, perhaps due to the compounding factor of Sinophobia during the pandemic. Another
possibility that could exist alongside the first is that TikTok, as a social media app, was much more accessible as a topic to the general public due to the threat being data collection and sharing, rather than the relatively more specialized concerns with Huawei’s relation to critical telecommunications infrastructure. Therefore, it would suggest that when an issue becomes highly technified over the course of its securitization, securitizing moves are more successful, though this warrants further study.

Indeed, the high saliency of the TikTok ban was likely driven not only by the relatively more accessible framing of the issue, but also due to its higher relevance to the population due to its large userbase, leading to more engagement and consideration of the securitizing arguments as well as more opposition to a ban. In fact, we found that the frequency with which individuals used an app strongly affected the effectiveness of securitizing arguments, with high frequency users of either app behaving much the same regardless of app, and non-users of either app being similarly distrustful after presented with an argument, whether or not securitizing elements were present. Since high frequency users of TikTok were not more affected by the arguments regarding TikTok’s untrustworthiness (whether from media or from directed securitizing arguments), any attempted government action regarding a highly relevant company or technology would be more difficult. Furthermore, as resulting trust for non-users of Instagram were as low as for non-users of TikTok, any technology with low relevance to users, regardless of whether it was securitized, would likely be viewed with suspicion when arguments regarding its malfeasance were presented. It appears then, that securitizing low-relevance technology may not be necessary for changing public opinion, but rather more important in legitimizing government action.
8.1 Questions and Concerns for Policymakers and the Public

These results present questions about US policy direction and framing of issues in the cyber realm. In cyberspace, we have now seen the broadly effective securitization of Chinese companies and the widespread and lasting acceptance of these arguments.

With the addition of cyber to the national security arena, the space for the US government to declare and act upon what it declares a threat has increased. With individuals and the data of Americans being possible components of US national security through the linkage of the individual to the network and the nation through grammars of cyber securitization, it legitimizes securitizing moves against entities that touch this data, whether they have threatening intentions or not. It allows the government to claim that these entities are existential threats with little justification by using technifying grammar and presenting it as relatively objective fact.

Even if, as our data suggests, the public’s lack of trust arose not only from the securitizing moves themselves but also the surrounding media coverage, overall trust of the securitized entities has nonetheless decreased. Having framed the issue as a threat to the US, the negative emotions appear to stand as a broad signal of audience acceptance of these narratives, even if the threat perceived for TikTok was due to mere wariness of general data collection, and not specifically Chinese data collection. Nevertheless, this suspicion of Chinese companies thus has moved public opinion to a place where the US government can then legitimize the actions it wishes to take against this alleged threat, which is the end goal of most securitizing moves taken by the political elite.

This type of securitization of China is nothing new in US policy. The TikTok ban is merely the current expansion and continuation of this trend. It was already successful with CNOOC and Huawei. It is currently continuing with artificial intelligence, and
we know not how far it may expand. If policy predicated on this kind of framing of China being a threat continues, particularly in areas that are relevant in the lives of so many Americans (such as social media and technology), it will only serve to further entrench connections between Chinese technology and suspicion and threat. The American populace do not necessarily have to buy the argument of China being an existential threat, so long as the connection, however latent, is created and made to exist that can be called upon to legitimized possible government action. This can only heighten tensions, exacerbate divides, and hamper collaboration and exchange.

8.2 Contributions and Future Directions

The relationship between politics and technology is a two-way street. Online presence has become ever more important in political campaigns, and social media has become in a sense parallel to traditional media, which has been seen as the “fourth branch of government.” However, political regulations and discourse also constrain and affect the ways in which the citizenry view and interact with technology. Thus, we believe it is important to examine the construction of these relations, particularly as nation-states have increasingly considered the cyber domain as part of national security, with individuals existing in cyberspace now ever-more intricately connected to these processes of securitization and political manoeuvring.

Therefore, in this work, we have focused on the concrete context, especially sociopolitical context, rather than hypotheticals. While evaluating general cues and factors that relate to trust is necessary and important, we also need to consider the real world developments and discourses that also may shape and shift user behaviour. Although prior work has shown that data collection and its associated risks are major factors in user assessments of privacy and trust, we have analyzed the particular sociopolitical factors that may affect these assessments and shape the awareness of
these risks. Though this work has focused on a particular securitizing narrative, that regarding TikTok, we believe that its findings can be applied to understanding securitizing moves more generally, as well as present one avenue of approaching the evaluation of political discourse on public opinion as relates to technology.

A nation is made of its people, and its political processes ought to be shaped through the participation and voices of the people. With the relatively unique affordances of cyber securitization, particularly through the technification grammar, it becomes ever more important for experts to step up and demystify these arguments. As the individual has become a referent object in these securitizing moves, and the results of everyday security practices and risk brought into the broader domain of national security, the individual in cyberspace has now become a key player in this field. It thus becomes critical that those with domain expertise share their knowledge to evaluate and present the arguments made about technology in a balanced manner that is understandable to general audience, in order that the public can evaluate the claims on their own merits rather than relying on biased claims that are presented as objective fact.

Technology may not inherently be a threat or a saviour, but it can be framed as either. Therefore, when political discourse and national security strategy drive its framing, it becomes ever more important to disentangle its component parts to understand what exactly is being propounded as the threat. Much like the Cold War Era, the United States can choose to continue to position a foreign nation as existentially threatening in cyberspace, and choose to continue simmering conflict. However, governments, as well as experts and the general public, can also choose to cooperate, and build towards a multilateral and global world made possible by the affordances of new technology rather than one divided by it. We simply have to decide which path to take. The clock is ticking, only this time, it is no longer an atomic clock, but a digital one.
Bibliography


[14] C. M.-Y. Cheung, C.-L. Sia, and K. K. Kuan, “Is this review believable? a study of factors affecting the credibility of online consumer reviews from an elm


[29] L. Hansen and H. Nissenbaum, “Digital disaster, cyber security, and the copen-


[53] Ministry of Information Technology, “Government bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of


u/bangorlol, “r/videos - comment by u/bangorlol on “not new news, but tbh if you have tiktiok, just get rid of it”,” Apr 2020. [Online]. Available: https://www.reddit.com/r/videos/comments/fxgi06/not_new_news_but_tbh_if_you_have_tiktiok_just_get/fmuko1m/


United States, Executive Office of the President [Donald Trump], “Executive Order 13873: Securing the Information and Communications Technology


Appendix A

Appendices

A.1 Survey

Users are shown the Apple Store icon of either TikTok or Instagram, then asked the following questions.

1. Have you used this app?
   - Yes
   - No
   - Not sure

2. How often do you use [TikTok/Instagram]?
   This question appears if “Yes” is selected for Question 1. One of the two apps in the brackets above appear, depending on the condition to which the respondent is randomized.
   - All the time
   - Several times an hour
   - Once an hour
• Several times a day
• Once a day
• Several times a week
• Once a week
• Several times a month
• Once a month
• Never

3. How trustworthy do you find the app [TikTok/Instagram]?

*This question appears if “Yes” is selected for Question 1. One of the two apps in the brackets above appear, depending on the condition to which the respondent is randomized.*

• Very trustworthy
• Somewhat trustworthy
• Neither trustworthy nor untrustworthy
• Somewhat untrustworthy
• Very untrustworthy

4. Have you heard about the app [TikTok/Instagram]?

*This question appears if “Yes” is not selected for Question 1. One of the two apps in the brackets above appear, depending on the condition to which the respondent is randomized.*

• Yes
• No
5. How trustworthy do you believe the app [TikTok/Instagram] to be, given what you may have heard about it?

This question appears if “Yes” is not selected for Question 1. One of the two apps in the brackets above appear, depending on the condition to which the respondent is randomized.

- Very trustworthy
- Somewhat trustworthy
- Neither trustworthy nor untrustworthy
- Somewhat untrustworthy
- Very untrustworthy

6. How much data do you believe [TikTok/Instagram] collects?

One of the two apps in the brackets above appear, depending on the condition to which the respondent is randomized.

- None
- Only what is necessary
- As much as these types of apps generally do
- Much more than necessary
- Everything it can

7. Please read the below paragraph carefully to answer following questions.

Participants then read one of eight short paragraphs, depending on the condition to which they were randomized.
• **TikTokAlarmistGovt** - TikTok, a popular social media app, has been under scrutiny for its data collection practices and alleged sharing of data with the Chinese government, and thus becoming a national security concern. TikTok is a data collection service that is thinly-veiled as a social network. If there is an API to get information on you, your contacts, or your device, TikTok is using it. According to experts, the app collects information such as phone hardware, the other apps you have installed, and everything network-related. This behavior may give the Chinese Communist Party access to Americans’ personal and proprietary information. It also encrypts all of its analytics requests with an algorithm that changes with every update to further obfuscate what they are doing. By contrast, the apps for Reddit and Twitter - which are both American companies - do not collect anywhere near the same amount of data that TikTok does. Due to these threats, some US departments have now banned TikTok from Federal Government phones.

• **TikTokNeutralGovt** - TikTok, a popular social media app, has been under scrutiny for its data collection practices and alleged sharing of data with the Chinese government, and thus becoming a national security concern. TikTok collects technical and behavioral information about your use of the app. According to experts, the app collects data that you provide, contact information, and device attributes. TikTok also collects information such as phone hardware, the other apps you have installed, and all network-related data. This behavior may also be shared with the Chinese government in response to law enforcement requests or government inquiries. The app also encrypts all of its analytics requests with an algorithm that changes with every update. TikTok, in general, collects more data than the apps for Reddit and Twitter - which are both American.
Due to these threats, some US departments have now banned TikTok from Federal Government phones.

- **TikTokAlarmistBase** - TikTok, a popular social media app, has been under scrutiny for its data collection practices. TikTok is a data collection service that is thinly-veiled as a social network. If there is an API to get information on you, your contacts, or your device, TikTok is using it. According to experts, the app collects information such as phone hardware, the other apps you have installed, and everything network-related. It also encrypts all of its analytics requests with an algorithm that changes with every update to further obfuscate what they are doing. By contrast, the apps for Reddit and Twitter do not collect anywhere near the same amount of data that TikTok does.

- **TikTokNeutralBase** - TikTok, a popular social media app, has been under scrutiny for its data collection practices. TikTok collects technical and behavioral information about your use of the app. According to experts, the app collects data that you provide, contact information, and device attributes. TikTok also collects information such as phone hardware, the other apps you have installed, and all network-related data. The app also encrypts all of its analytics requests with an algorithm that changes with every update. TikTok, in general, collects more data than the apps for Reddit and Twitter.

- **InstaAlarmistGovt** - Instagram, a popular social media app, has been under scrutiny for its data collection practices. It may be deceiving users about their ability to control the privacy of their personal information, as there is often no meaningful consent or understanding of what user data can be used for or which entities it may be shared with, such as the US government. Instagram is a data collection service that is thinly-veiled as a
social network. If there is an API to get information on you, your contacts, or your device, Instagram is using it. According to experts, the app collects information such as phone hardware, the other apps you have installed, and everything network-related. This behaviour by Instagram may give the US government access to your personal and proprietary information. It also encrypts all of the analytics requests with an algorithm that changes with every update to further obfuscate what they are doing. By contrast, the apps for Reddit and Twitter do not collect anywhere near the same amount of data that Instagram does. Due to these threats, some governments have now banned Instagram from military personnel’s devices.

- **InstaNeutralGovt** - Instagram, a popular social media app, has been under scrutiny for its data collection practices. It may be deceiving users about their ability to control the privacy of their personal information, as there is often no meaningful consent or understanding of what user data can be used for or which entities it may be shared with, such as the US government. Instagram collects technical and behavioral information about your use of the app. According to experts, the app collects data that you provide, contact information, and device attributes. Instagram also collects information such as phone hardware, the other apps you have installed, and all network-related data. The data collected by Instagram may also be shared to respond to law enforcement requests or US government inquiries. The app also encrypts all of its analytics requests with an algorithm that changes with every update. Instagram, in general, collects more data than the apps for Reddit and Twitter. Due to these threats, some governments have now banned Instagram from military personnel’s devices.

- **InstaAlarmistBase** - Instagram, a popular social media app, has been
under scrutiny for its data collection practices. Instagram is a data collection service that is thinly-veiled as a social network. If there is an API to get information on you, your contacts, or your device, Instagram is using it. According to experts, the app collects information such as phone hardware, the other apps you have installed, and everything network-related. It also encrypts all of the analytics requests with an algorithm that changes with every update to further obfuscate what they are doing. By contrast, the apps for Reddit and Twitter do not collect anywhere near the same amount of data that Instagram does.

- **InstaNeutralBase** - Instagram, a popular social media app, has been under scrutiny for its data collection practices. Instagram collects technical and behavioral information about your use of the app. According to experts, the app collects data that you provide, contact information, and device attributes. Instagram also collects information such as phone hardware, the other apps you have installed, and all network-related data. The app also encrypts all of its analytics requests with an algorithm that changes with every update. Instagram, in general, collects more data than the apps for Reddit and Twitter.

Participants are then asked, “Given the information presented on the previous page (and shown again below), please answer the following questions.”

8. Given the information presented, how trustworthy do you find the app [TikTok/Instagram]?

One of the two apps in the brackets above appear, depending on the condition to which the respondent is randomized.

- Very trustworthy

- Somewhat trustworthy
• Neither trustworthy nor untrustworthy

• Somewhat untrustworthy

• Very untrustworthy

9. Given the information presented, how much data do you believe [TikTok/Instagram] collects?

One of the two apps in the brackets above appear, depending on the condition to which the respondent is randomized.

• None

• Only what is necessary

• As much as these types of apps generally do

• Much more than necessary

• Everything it can

10. What nationality is the [TikTok/Instagram] app?

Please enter your best guess, answers such as “None” or “I don’t know” will not be accepted.

For this question, respondents write a free-response answer in a text-box

11. Do you work in the tech industry or have you studied computer science or a related field?

• Yes

• No

12. What is your current age?
13. How would you describe your political views on social issues?

- Very socially liberal
- Somewhat socially liberal
- Neither socially liberal nor socially conservative
- Somewhat socially conservative
- Very socially conservative

14. How would you describe your political views on economic issues?

- Very economically liberal
- Somewhat economically liberal
- Neither economically liberal nor economically conservative
- Somewhat economically conservative
- Very economically conservative
A.2 Reddit Comment

Below is reproduced the text of the Reddit comment posted by u/bangorlol on April 8, 2020 in the r/videos subreddit under the post “Not new news, but tbh if you have tiktok, just get rid of it” linked to a YouTube video that has now been deleted. The comment has over 28k karma and over 140 awards.

So I can personally weigh in on this. I reverse-engineered the app, and feel confident in stating that I have a very strong understanding for how the app operates (or at least operated as of a few months ago).

TikTok is a data collection service that is thinly-veiled as a social network. If there is an API to get information on you, your contacts, or your device... well, they’re using it.

Phone hardware (cpu type, number of course, hardware ids, screen dimensions, dpi, memory usage, disk space, etc)

Other apps you have installed (I’ve even seen some I’ve deleted show up in their analytics payload - maybe using as cached value?)

Everything network-related (ip, local ip, router mac, your mac, wifi access point name)

Whether or not you’re rooted/jailbroken

Some variants of the app had GPS pinging enabled at the time, roughly once every 30 seconds - this is enabled by default if you ever location-tag a post IIRC

They set up a local proxy server on your device for ”transcoding media”, but that can be abused very easily as it has zero authentication

The scariest part of all of this is that much of the logging they’re doing is remotely configurable, and unless you reverse every single one of their
native libraries (have fun reading all of that assembly, assuming you can get past their customized fork of OLLVM!!!) and manually inspect every single obfuscated function. They have several different protections in place to prevent you from reversing or debugging the app as well. App behavior changes slightly if they know you’re trying to figure out what they’re doing. There’s also a few snippets of code on the Android version that allows for the downloading of a remote zip file, unzipping it, and executing said binary. There is zero reason a mobile app would need this functionality legitimately.

On top of all of the above, they weren’t even using HTTPS for the longest time. They leaked users’ email addresses in their HTTP REST API, as well as their secondary emails used for password resets. Don’t forget about users’ real names and birthdays, too. It was allllll publicly viewable a few months ago if you MITM’d the application.

They provide users with a taste of ”virality” to entice them to stay on the platform. Your first TikTok post will likely garner quite a bit of likes, regardless of how good it is.. assuming you get past the initial moderation queue if thats still a thing. Most users end up chasing the dragon. Oh, there’s also a ton of creepy old men who have direct access to children on the app, and I’ve personally seen (and reported) some really suspect stuff. 40-50 year old men getting 8-10 year old girls to do ”duets” with them with sexually suggestive songs. Those videos are posted publicly. TikTok has direct messaging functionality.

Here’s the thing though.. they don’t want you to know how much information they’re collecting on you, and the security implications of all of that data in one place, en masse, are fucking huge. They encrypt all of the analytics requests with an algorithm that changes with every update
(at the very least the keys change) just so you can’t see what they’re doing. They also made it so you cannot use the app at all if you block communication to their analytics host off at the DNS-level.

For what it’s worth I’ve reversed the Instagram, Facebook, Reddit, and Twitter apps. They don’t collect anywhere near the same amount of data that TikTok does, and they sure as hell aren’t outright trying to hide exactly what’s being sent like TikTok is. It’s like comparing a cup of water to the ocean - they just don’t compare.

tl;dr; I’m a nerd who figures out how apps work for a job. Calling it an advertising platform is an understatement. TikTok is essentially malware that is targeting children. Don’t use TikTok. Don’t let your friends and family use it.