Andrew Buzzell University of Western Ontario
Owen Chevalier University of Western Ontario
Lucas Pokrywa University of Western Ontario
Jacquelyn Burkell University of Western Ontario

TikTok as a Threat to Democracy? Conceptions of Cognitive and Epistemic Security in Discourse on the TikTok Ban

"A foreign government messing around in our elections is, I think, an existential threat to our way of life. To me, and this is to me not an overstatement, this is the political equivalent of 9/11"

> Fmr. CIA Acting Dir. Michael Morell speaking about Russia's social media information operations to influence American voting behaviours during the 2016 US election (Morell, 2016)

Introduction

In many countries there have been calls to ban or regulate the social media platform TikTok because of national security concerns with the app. These concerns, often loosely defined, include the risk conventional espionage and surveillance that could be enabled by the app installed on government devices. Another category of security concerns evident in policy discourse about TikTok and reflected in the opening quote from the Acting Director of the CIA is that it poses a national security risk because it affords the Chinese government a dangerous means of interference with democratic information environments. There is worry that the platform might be used to manipulate individuals and groups, to interfere with public opinion and elections, used as a vector for propaganda and disinformation, and/or to censor and shape the information environment to further the strategic objectives of the Chinese government. This collection of concerns undermines what has been labelled *cognitive security* (Waltzman, 2017) - a term that has gained currency in national security policy discourse, alongside related terms including "cognitive warfare".

Although the general thrust of the policies is clear – to protect the public against malign influence on knowledge, attitudes, and behaviour – the mechanisms of threat against which the policies are designed to protect are much less clear. Strong and effective policy requires conceptual clarity (De Campos, 2020; Kubrin, 2008). Until and unless we clarify the problems that policies are designed to address, we are hampered in producing good policy. In

the case of TikTok, this category of motivating concerns is poorly specified. If TikTok poses some kind of threat to the cognitive security of democracies, what is it exactly?

We address this question through Bacchi's 'what is the problem represented to be' (WPR) approach to policy analysis (Bacchi, 2012), which fits well with contemporary securitization theory and its constructivist approach to threat identification and analysis (Balzacq, 2009; Buzan & Wæver, 1997). We apply this analytic approach to policies and policy discussions regarding the TikTok ban/divesture legislation in the United States (H.R.7521, 2024), focusing on the issues or problems as represented in those policies and policy discussions. These analyses provide a comprehensive overview of the perceived cognitive threats presented by this platform as identified in policy discourse and legislation. We identified seven problem representations that relate to the cognitive security risk of TikTok, but two stand out in terms of both occurrence and salience. The first is that the risk is based on the ownership and control of the platform by a hostile foreign adversary, China. The second is that the cognitive security risk stems from the data collection and processing activity of TikTok. Policies oriented to these representations do not directly address the cognitive and epistemic concerns that we find intertwined with them in policy discourse. In our analysis of these motivations, we find that targeting TikTok's data collection and ownership is likely to have limited success. If these motivations are legitimate policy objects, then research and policy innovation should consider them directly. The extent to which these ideas have percolated into public policy discourse is also significant as it entices politicians to highlight these concerns in the legislation they propose and support (and that which they oppose).

1. Background – influence and manipulative security threats and TikTok

Many jurisdictions have enacted, or are considering, bans on TikTok. The United States recently passed bill H.R.7521 - Protecting Americans from Foreign Adversary Controlled Applications Act, which will ban TikTok unless it is divested to an American-controlled company. Taiwan is considering expanding its public sector ban on TikTok into the private sector over concerns about China's "cognitive warfare" (LaMattina, 2024; Sang et al., 2024), and other countries, including India, as well as China itself, have banned the app within their national cyber-borders.

Worries about TikTok's ability to collect and process personal data about users and the content they produce and consume within the app are salient in these policies (Anja Karadeglija, 2022; Martina & Shepardson, 2023). The underlying concerns often relate to how this data might be used— that these might be leveraged by the Chinese government to influence opinions, attitudes, and even behaviours of TikTok users in ways that undermine democracy. A 2023 briefing note from Canada's department of public safety warns that TikTok may "... undermine democratic values and exert foreign influence" (Public Safety Canada, 2023), and cites the US FBI Director Christopher Wray's warning that China has

control over TikTok's recommendation algorithm, "... which allows them to manipulate content, and if they want to, to use it for influence operations." (Wray, 2022)

These concerns are not unfounded. Election interference, for example, which is a common worry in the background of TikTok policy, can take on a variety of forms. Hack and leak operations, as occurred with the Podesta emails during the 2016 US election (McKay & Tenove, 2020), rely on domestic audiences freely circulating what is often true information, though such operations are frequently supplemented with forgeries and efforts to reframe and recontextualize the content using bots and paid human actors, which is then reflected and amplified by genuine accounts. Fake news, deep fakes, and other forms of misinformation and disinformation are often accompanied by efforts to control the salience and suggest interpretations of the content in the hope that real users will engage and endorse. During the 2023 Taiwanese election, Chinese disinformation tactics supplemented specific examples of faked and false evidence of waning US support with more general messaging efforts to increase scepticism about the US as a reliable ally and worry about US abandonment of Taiwan (Köckritz, 2023). During the initial phases of the COVID-19 pandemic, researchers found that TikTok was a particularly prominent source of misinformation and disinformation, some of which did not involve specific false claims but instead aimed to frame aspects of the pandemic and public health response in partisan terms (Basch et al., 2021; Southwick et al., 2021).

Some concerns about TikTok's ability to influence public opinion and voting behaviours stem from belief that China is capable using TikTok's recommendation algorithms for both overt censorship and covert influence. As with all social media platforms, TikTok does afford a capacity for censorship that can affect political attitudes and behaviour, but important questions about how it works and how it is used are impossible to answer from public sources. Douyin, the domestic version of TikTok available in China (where TikTok itself is banned), has moderation and recommendation systems which are explicitly tasked to amplify content that promotes the state vision of patriotic "positive energy" (Yang & Tang, 2018). It also demotes and removes content the state deems sensitive. In a recent report, the University of Toronto's CitizenLab found that "[a]cross eight China-accessible search platforms analyzed — Baidu, Baidu Zhidao, Bilibili, Microsoft Bing, Douyin, Jingdong, Sogou, and Weibo — we discovered over 60,000 unique censorship rules used to partially or totally censor search results returned on these platforms." (Knockel et al., 2023). The rise of "algospeak" among TikTok users, to get around automated filters that ban terms like suicide, Tiananmen square, abortion, by using words like "unalive", "May 35", and "going camping", demonstrates both the creative efforts of users to avoid automated censorship, and also helps to reveal kinds of content users have experienced frustration trying to post and share. Sometimes China has attempted to block content indirectly, by flooding the media environment with similar hashtags and misusing popular hashtags, to impede organic discovery, such as the massive repetition of city names in banal postings on Twitter during the pandemic to frustrate communication about infection rates. (McBride et al., 2020; Milmo & Davidson, 2022)

Unlike many social media platforms which prioritize content from a user's social graph, TikTok's feed is primarily driven by the recommendation system which models user preferences and produces the app's "For you" page, the primary mode of content discovery. Beyond outright censorship, there are worries that TikTok's recommendation algorithm affords influence over the atmosphere of public opinion and even afford the means to indirectly shape downstream voting behaviour. For example, researchers in the US found that videos from get-out-the-vote campaigns were poorly ranked and possibly suppressed for some demographics (Murray 2022). In late 2023, Osama Bin Laden's "Letter to America" began to trend on TikTok, primarily to younger audiences, and framed in connection to the October 7, 2023, Hamas-led attack on Israel and Israel's subsequent response. Amid concerns raised in the US about "indoctrination" and suspicion that the Chinese government sought to weaken American support for Israel, TikTok was pressured to censor the #lettertoamerica hashtag (Helberg, 2023; Lakomy, 2024). Many worried that interest in the video was nudged not by some nascent interest but by the recommendation system itself, possibly at the direct command of China. Some found it distressing that a cohort of American youth born after 9/11 espoused solidarity and sympathy with Bin Laden (Baker-White, 2024), and yet expressions of this concern, especially by officials, was inescapably symbolic. Views of the video didn't exceed 15 million, a small number given the scale of the platform and the idiosyncrasies of its analytic systems (e.g., the most watched TikTok videos of 2023 amassed view counts between 357 million and 2.3 billion. (Ceci, 2024))

These examples are consistent with China's military doctrine on cognitive and information warfare, often referred to as cognitive domain operations, which combine "... psychological warfare with cyber operations to shape adversary behaviour and decision making", to serve as an " ... offensive capability to shape perceptions or polarize a society" (Office of the Secretary of Defense, 2023, p. 156) A distinctive aspect of cognitive warfare is that it adopts broader aims than conventional information operations, which seek the promulgation of a specific message, to instead alter the broader conditions of sensemaking and interpretation - "... the orientation of the context literally is the contest" (Rogers, 2021, p. 87). Russia's use of the "firehose of falsehood" (C. Paul & Matthews, 2016) strategy to overwhelm an information system with competing narratives to exhaust the audience and reduce trust in the environment as a whole is an example of a technique that is cognitive more than informational (Claverie & Du Cluzel, 2022; Hersch et al., 2024).

2. Constructing cognitive security and insecurity

From this sketch we can see a range of justifications for the idea that TikTok poses a national security threat to countries in conflict and competition with China and its allies in part because of its affordance of various capabilities to influence, shape, and structure information environments inside democracies. But despite how frequently these worries are found

together in policy discussions, they are in fact quite heterogenous and can be assembled in a variety of competing and conflicting configurations and interpretations.

This broader category of concerns about influence, manipulation, censorship, and malfeasance in the information space we can subsume under the banner of "cognitive security", a term that has gained some currency in national security discourse (alongside the concomitant rise of the concept of "cognitive warfare") (Claverie & Du Cluzel, 2022; Hersch et al., 2024; Hung & Hung, 2022). It denotes security vulnerabilities that, while they often accidentally overlap with cyber, economic, biological and other security concerns, are of their own distinct kind, and which involve a "...qualitatively new landscape of influence operations, persuasion, and, more generally, mass manipulation" (Waltzman, 2017 p. 2) or what communication scholars Robert Gehl and Sean Lawson call "mass personal social engineering (Gehl & Lawson, 2024). While use of the term is still relatively uncommon, its conceptual content appears in many articulations of concern about various kinds of weaponization of media and information systems. From this perspective, calls to ban or regulate TikTok because of national security concerns about various forms of malign and destructive influence can be understood as invoking a conception of cognitive security. This invites us to critically examine exactly how specific policy proposals are constructing this notion of security and perceived risks and vulnerabilities.

Our analysis is based on Carol Bacchi's "What the problem is represented to be" framework (Bacchi, 2009, 2012; Bacchi et al., 2016). This approach analyzes policy in terms of how it construes and constructs the problems it aims to solve, rather than taking its problematic as given and analyzing the policy as potential solution. Here we examine the different ways that features and properties of TikTok are constructed as threats to security that in turn motivate policy advocacy. Citing Cox (1981) Bacchi observes that "problem-solving approaches are by their nature conservative" (Bacchi, 2009), in that they imagine the problem as an aberration against a background of normal functioning. In the context of security and securitization, problem-solving approaches invite a conception of the threat as a deviation in an otherwise functional or stable state of affairs. We imagine some forms of state security just as freedom from violent conflict, from losing territory, and so forth. In the domain of computer security, we can delineate categories of abuse and unauthorized access against a background of relatively stable understandings of what systems are for, what they are supposed to do, and who is supposed to use them.

When we are talking about online media and speech environments, it is far more difficult to identify the ‘proper normal functioning’ that policies would aim to protect or return to. We don't imagine these systems only produce truths, that they require particular authorizations, credentials, or approvals, that they have pre-ordained purposes, and so forth. Where cybersecurity seeks to reduce trust, our social epistemology depends on it irreducibly - we cannot constantly interrogate all the information we receive from others, nor the infrastructural and material conditions of its transmission. It is particularly difficult to describe a normal state of the rapidly changing media environment, or to assess its health.

Attempts in policy often resort to terms such as "organic", "authentic", "resilient", "trustworthy" - that themselves contain implicated but unarticulated normative content. Goals pursued by policy motivated by cognitive security concerns include protecting individuals, communities, and states in a future where "researchers, governments, social platforms, and private actors will be engaged in a continual arms race to influence" (Waltzman, 2017 p. 7). However, it is critical to the public interest that, whatever conceptions of gains and losses are mobilized in this arms race, particularly by democracies enacting defensive policy, these reflect our best theoretical understandings of what kinds of protection is needed, and in what ways that protection can be effectively, ethically, and legally pursued.

Therefore, when we find that conceptions of cognitive security appear to motivate some policy, we should be especially wary about their adequacy, their theoretical and empirical basis, and implicated ideals about how free and democratic information spaces are supposed to work. Here we take up Bachii's method because it explicitly alerts us to uncertainty and arbitrariness in specific constructions of security, and aims to make it possible to "... 'work backwards' from a proposal to how a 'problem' is represented - to 'read off' the problem representation from the proposal or proposed solution" (Bacchi et al., 2016 p. 18).

The primary critical aim here is not the assessment of policy itself, but instead to make the assumptions and concepts underlying policy available for assessment. In the broader context of critical security studies, security threats are "...staged as existential threats to referent objects by a securitizing actor who thereby generates endorsement of emergency measures beyond rules that would otherwise bind" (Buzan et al., 1998 p. 5), and can thus be interrogated as constructions that embed and reproduce conditions favoured by the securitizing actor. In the case of TikTok, the "rules that bind" include norms about free speech, journalism, domestic public diplomacy, and access to information in liberal democracies, and the referent objects not just media platforms and media professionals, but the epistemic and cognitive activity of everyday citizens.

We engage a variety of policy documents in this analysis to understand how notions of cognitive security are constructed and mobilized in the articulation of reasons to ban or regulate TikTok as a threat to national security. Our use of WPF is motivated by a desire to uncover underlying and implicit assumptions about psychological, social and political epistemological concepts relating to political and intellectual autonomy, manipulation, and influence, assumptions about the technological manifestations of risks to these, and connections to legal and ethical norms, that are assumed in constructions of the threat of TikTok and social media that then become the object of policy making.

3. Methodology: what the problem is represented to be

We analysed documents in legislative, academic, and policy discussions of the security threat posed by TikTok to identify significant and recuring narrative, conceptual, and thematic

content expressing ideas about epistemic and cognitive security. We began with hand selection of key policy documents, especially in the context of the 2024 H.R.7521 - Protecting Americans from Foreign Adversary Controlled Applications Act, and preceding legislative initiatives in the US. Search terms were developed to capture a broad range of discourse surrounding TikTok and national security and were derived both inductively (from initial exploratory searches) and deductively (based on concepts identified in existing literature and policy documents). Our inclusion criteria limited results to documents in English, from legislation, academic articles, policy documents, government reports, think tank publications, and reputable media articles, which included problem representations that related to cognitive security concerns. This excluded documents focussed solely on cyber-related security concerns, surveillance risks and espionage, as well as those motivated by more general social concern for harms such as hate speech, illegal content, dangerous content, and addiction. Our search was purposive – to sample the region of discourse that involves broadly construed concerns about influence and manipulation of the information environment. Documents were limited to the period between 2018 and the present when TikTok's popularity surged and when concerns about its impact became prominent.

The document search was conducted using academic databases (Google Scholar, JSTOR, Scopus), policy databases (ProQuest, Policy Commons, government websites), and media archives (Nexis Uni). The search was iterative, and initial searches were used to refine terms and identify additional relevant concepts. We used the Covidence software platform to screen documents based on titles and abstracts to determine relevance according to the inclusion criteria. Our initial search yielded 423 documents. On the basis of title screening, 167 documents were selected for full text screening, and of these 57 were selected for data extraction. Title screening excluded documents that had identical titles, or were duplicate reporting of the same primary content, if they were not published in a prominent venue, or not published in English, or not available to access. From full text screening to extraction, documents were also excluded for these reasons, but also if they did not include a substantive problem representation with some connection to cognitive and epistemic security concerns broadly construed.

We conducted data extraction using deductive coding of problem representations we identified from key documents. We started with an initial deductive set of coding criteria and added new ones as we reviewed documents and discovered new representations of the problem.

3.1 Problem representations

Problem representation	What's the problem?	Example

Censorship	TikTok can censor content and stifle free expression to suppress information and opinion China views unfavourably.	"TikTok, the popular Chinese-owned social network, instructs its moderators to censor videos that mention Tiananmen Square, Tibetan independence, or the banned religious group Falun Gong, according to leaked documents detailing the site's moderation guidelines." (Hern, 2019)
Propaganda	TikTok is a vehicle for distributing propaganda	"Communist China is using TikTok as a tool to spread dangerous propaganda that undermines American national security" (House Select Committee on the Chinese Communist Party, 2024)
Influence	TikTok can use its AI powered recommendation algorithm misrepresent the salience of views, content, and framings, to shape of mass opinion.	"While there are several major Canadian media outlets on TikTok…these outlets simply cannot compete with TikTok's algorithm when the PRC intends to manipulate the information space" (Lee, 2024).
Data Collection	TikTok collects, scavenges and hoards personal data for future dangerous use to influence or manipulate (distinct from espionage risks)	"Congress is pursuing the legislation over national security concerns about the Chinese government's access to U.S. user data and its ability to conduct influence campaigns through the platform." (Knuston, 2024)
Socially and Politically Dangerous	TikTok algorithms are dangerous socially (polarization, demoralization, extremism, etc)	"Since many viewers won't realize the videos are part of a targeted disinformation campaign, it greatly enhances the effectiveness of IOs to sow confusion, polarize public debate, and fuel extremism" (Lee 2024)

Epistemic pollution	TikTok is designed and managed in ways that foster mis/dis/mal information (including deep fakes, fake accounts, etc)	"TikTok has also proliferated misinformation on a number of other political subjects. Infamously, TikTok facilitated the spread of misinformation regarding COVID-19, from vaccines to treatments, and on a wide range of other topics, such as climate change." (Patnaik & Litan 2023)
Hostile ownership	TikTok is dangerous because it is controlled by a hostile foreign adversary.	"TikTok is not the first company with ties to China to face scrutiny. For example, the United States has banned Chinese companies such as Huawei over national security concerns. Washington has denied necessary equipment approvals to some businesses, placing them on a "covered list" of companies viewed as a threat to the security of America's telecommunications infrastructure." (Huddleston, 2023).

Finally, we analysed the representations following the Bacchi's "what the problem is represented to be" (WPR) method and then synthesized the findings to draw conclusions about the concerns underlying the policies and public discourse surrounding the TikTok ban.

4. Analysis

Our analysis is based on the four core steps of Bacchi's framework. We have omitted steps three "How has this representation of the 'problem' come about?" and six "How/where has this representation of the 'problem' been produced, disseminated and defended?", which emerged in later iterations of Bachi's framework, and are intended to elicit the historically contextualized power relations that shape problem representation. This is a useful direction for future research but beyond our scope. The outputs of Bacchi's first step, the identification of problem representations, are collected in table in Section 3.1. Here then, we turn to analyze these problem representations using the remaining three steps of WPR (Bacchi, 2009):

Identify the presuppositions or assumptions which underpin representation of the 'problem'
The objective of this step is to identify implicit and explicit ideas about what the problem is.

Identify what is left unproblematic in this problem representation
The objective of this step is to identify important unaddressed elements of problem representations.

What effects are produced by this representation of the 'problem'?
The objective of this step is to identify the actual and probably policy ideas that are suggested and constructed by the problem representation

4.1 Hostile Ownership

For many policymakers, the problem with TikTok is primarily that it is operated by a foreign adversary. In the United States, China is designated as an adversary, which has "... engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States person" (15 CFR 791.4, 2024) Almost every mainstream social media platform: Meta (Facebook, Instagram, WhatsApp), Snapchat, X (formerly Twitter), Alphabet (which owns YouTube), is based in the US.

TikTok itself is owned by a Chinese company, ByteDance, and is subject to national laws such as the National Intelligence Law of 2018 and the Chinese Cybersecurity Law of 2016, which compel companies to cooperate with state security officials. In addition, the Chinese government has control over ByteDance by way of a "golden-share," which gives some measure of financial and decision-making power over the company to a state actor, in this case the China Internet Investment Fund, which is operated by China's Cyberspace Administration, and has been described as a "... [s]word of Damocles hanging over the heads of firms that have them" (Aho, 2023).

Policy discourse and legislation frequently securitizes the mechanisms and affordances of TikTok on the basis of the risks they pose if China is able to use them with hostile intent. The titles of recent legislative proposals in the US reflect this:

> Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and the Algorithmic Learning by the Chinese Communist Party Act (H.R. 1081/S. 347)
>
> The Stopping Attempts by Foreign Entities to Target Youths on Social Media Act of 2023 (S. 872)

Deterring America's Technological Adversaries (DATA) Act (H.R. 1153)

Protecting Americans from Foreign Adversary Controlled Applications Act (H.R.7521)

Worries about TikTok and its affordance of propaganda, influence, surveillance, censorship, are typically articulated in relation to the status of the platform owner as a foreign adversary.

Presuppositions or assumptions which underpin representation of the 'problem'

There are two linked assumptions that are important in this problem representation. Firstly, that the security risks of TikTok have a causal relationship to the ownership of the platform by a Chinese company. The problem is represented as a risk of damage China can do to US national security because it controls TikTok.

Secondly, that these risks attach to the controllers of the platform, not to its sociotechnical design, its affordances to other users, or its role in the broader media ecology – that a TikTok in American hands is safer from a security perspective. If TikTok's security threats arise because it is operated by a Chinese company, then solutions targeting this, such as divestiture, appear as obvious policy options.

What is left unproblematic in this problem representation

Security risks from US controlled platforms, and from hostile actors other than China, are both left unproblematic in this way of framing the security risk of TikTok. Many of the worries that arise in this policy discussion apply equally to other state actors, and to other platforms. Russia has extended its long running information campaigns onto the TikTok platform, spreading propaganda and disinformation relating to its invasion of the Ukraine (Evans, 2022), a conflict that has been called the first "TikTok war" (Chayka, 2022). Other platforms, such as Meta and YouTube, have recently blocked several Russian state-affiliated broadcasters from their services (K. Paul, 2024). But content with origins in their media ecosystem, often coordinated on other platforms like Telegram, still circulates freely (Gursky et al., 2022). Iran has also recently been implicated in efforts to use social media platforms to influence the 2024 US presidential election (Bond, 2024) and, has engaged information operations in support of Hamas on social media platforms including TikTok (Dostri, 2024), but also, on China's internal version of TikTok, Douyin (Brar, 2023), with the tacit approval of the Chinese government.

Increasingly, even non-state actors can use social media platforms to engage in private deceptive and manipulative information operations, even to influence elections, and can have substantial impacts on public opinion (Woolley, 2023). This leads to second bundle of issue

that are left unproblematic – that security risks might not arise because of who owns the platforms, but because some kinds of action they afford, to anyone, given the time, motives, and resources. Concerns about hostile ownership, and data collection, are frequently proxies for other motivating worries about influence and manipulation of information environments that social media platforms afford. We have a more limited theoretical, empirical, and legal basis to act on these. In America, where most social platforms are headquartered, and where TikTok will be if the H.R. 7521's deadline is reached, legal protections of speech and speech intermediaries, which currently regards recommendation and moderation systems as protected expressive activity, limits current direct policy options.

Effects produced by this representation of the 'problem'

A primary effect of this framing is to focus policy debate on the norms around foreign investment and business operation, especially as they relate to speech and expression. When anchored to its Chinese ownership, regulation of TikTok that would reduce or eliminate its US presence can appear to regulate a speech environment just because of some fact about the identity of the operator. A secondary effect is the extent to which the framing directly entails a policy solution that leaves unaddressed the mechanisms involved, and instead addresses the likelihood of a hostile actor realizing them.

Many of the concerns raised about TikTok in policy discourse are expressed in the language of risks and hypotheticals, (or lack unclassified evidence). Even if we should accept a framing of the problem focussed on the PRC as a hostile adversary, as we will discuss in the next section, it does not need to control TikTok to access US data or conduct information operations and cognitive warfare. If what makes social media platforms like TikTok an object of security concern has more to do with how the platforms work than with who owns them, then the need for serious investment in policy innovation is left unproblematic by this representation of problem.

4.2 Data collection and processing

Setting aside concerns about data collection as a means of espionage, we can identify two distinct problem representations related to TikTok's collection and processing of personal data: coercion and microtargeted persuasion and influence.

Data driven coercion

The coercive threat is based on concerns that the data collected might be used in a more conventional targeted influence campaign, providing the means to coerce specific individuals. TikTok's data holdings can help China "...uncover the vices, predilections or pressure points of a potential spy recruit or blackmail target, or by building a holistic profile of foreign visitors to the country by cross-referencing that data against other databases it holds" (Fung,

2023). This particular problem representation can be found in previous policy, such as the Committee on Foreign Investment in the United States (CFIUS) action in 2019 to compel a Chinese consortium to divest ownership of the dating app “Grindr". CFIUS applied new regulations developed in 2018, the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018, which permits CFIUS intervention in cases where there is a risk of exposing “personally identifiable information, genetic information, or other sensitive data of United States citizens to access by a foreign government or foreign person that may exploit that information in a manner that threatens national security” (FIRRMA 1702(c)(5)). Thresholds for action include the possession of data on over 1 million users, or where the company has a “demonstrated objective” of undermining US national security, or where there is a risk of “... a foreign government gaining a significant new capability to engage in malicious cyber-enabled activities against the United States, including such activities designed to affect the outcome of any election for Federal office.” (FIRRMA 1702(c)(6)) In the cases of Grindr, while CFIUS did not release its reasoning to the public, reporting suggested that there were concerns about the use of the data to bribe or manipulate specific individuals, particularly military service members.

It’s arguable that this problem representation falls outside the category of the cognitive and epistemic, given its reliance on brute forms of fear and coercion rather than indirect influence. However, when deployed at scale to exert psychological coercion in groups, the line is blurred. For example, Russia sent bulk SMS messages to Ukranian soldiers and their families during the 2018 invasion of the Donbass, telling families of service members that they had been killed, and soldiers they were surrounded (Collines, 2018), and similar more recent examples can be found during the conflict in Gaza (Weimann & Weimann-Saks, 2024) where targeted messages sought to weaken morale.

Consider TikTok’s dark-pattern lobbying campaign targeting US users – where the app itself appeared to be unusable and users were induced to use a button on the screen to call their political representatives to object to the proposed ban, flooding phone systems. This did little to assuage worries that TikTok can manipulate the political behaviour of its users (Wu, 2024) and demonstrated it's capacity to spur political action in its userbase. A Brookings institute report articulates the problem clearly:

> “Content uploaded to the Chinese-owned viral video app Tiktok, for example, could be used to develop a model of service members who are expressing discontent, are susceptible to influence operations, or could be recruited by Chinese spies (perhaps with the help of purloined travel data). The vulnerability lies not in any individual piece of data but the ability to aggregate it and draw inferences from it that can be weaponized against the United States and its allies.” (Dawson & Wheeler, 2022)

Note the way in which concerns about individual coercion and blackmail, which are not distinctively cognitive and epistemic, are mixed here with concerns that are. This is because they share underlying worries about mechanisms and hostile intentions. An important

question arises, how much data do you really need to craft and circulate persuasive messaging of the sort the report worries might influence unhappy US service members?

Data-driven persuasion

The second problem representation involves the use of TikTok's data holdings to support propaganda and disinformation campaigns. Both mobilize worries about the data TikTok has about users and the extent to which this can be used to construct and deliver persuasive messaging. The microtargeting threat is grounded in the observation of how engaging, even addictive, the TikTok algorithm is, which reflects its ability to model individual preferences and psychology. Clearly TikTok knows its users well. Concern about the potency of microtargeted persuasion is not new (Barocas, 2012; Hersh, 2015) but as empirical evidence has accumulated, support for its effectiveness is mixed, and generally weak. A recent study casts doubt on its efficacy in political contexts, finding that messaging and targeting based on a single datapoint performed as well as microtargeted efforts (Tappin et al., 2023).

Elections raise heighted interest in microtargeting as data-driven campaigning have become increasingly commonplace (Roemmele & Gibson, 2020), and widely viewed as potentially decisive, allowing political campaigns to deliver "personalized messages to individual voters by applying predictive modelling techniques to massive troves of voter data "(Rubinstein, 2014). However, a recent study of democratic states where data-driven campaigns have been deployed raises doubts, finding that targeting and messaging, even when stategies espoused and adverted to use microtargeting, were in fact conducted by conventional means. (Kefford et al., 2023).

Finally, there are risks that TikTok may use its vast data holdings to improve its ability to produce effective disinformation (Lavoy, 2024) while shielding it from other entities that might wish to train on the same data.

Presuppositions or assumptions which underpin representation of the 'problem'

There is an assumption that data collected by TikTok affords the Chinese government a unique source of information about US persons, which elevates the risks of both the coercive and microtargeting problem. Forced divestiture addresses this assumption by forcing TikTok to transfer ownership to US controlled entity, and TikTok's "Project Texas", offered as a compromise on this point, included plans to maintain US data within data centres on US soil and avoid its transmission outside the US, as well as transferring control of US operations to an entity with direct CFIUS oversight.

There is an underlying assumption that TikTok's data holdings are the primary vector for a more disparate range of cognitive concerns, those related to influence, censorship, and disinformation propaganda. Combined with the problem of control by China, a hostile foreign

adversary, this motivates solutions that imagine cutting of China's supply of US data will mitigate the threats.

What is left unproblematic in this problem representation

Concerns about the use of personal data collected by TikTok to target influence campaigns depend on assumptions about the risks foreign control, that there's something particularly dangerous about the possibility of access to data that ByteDance's relation to the Chinese state affords. As we find it in policy discourse, the problem of data collection and processing is entangled with the problem of Chinese ownership, and a complex of concerns about possible actions involving influence and information control. But if we think access to data by an adversary is the threat, then this overlooks tools offered by TikTok, but also by other platforms which make available to a variety of users (such as content creators and advertisers) the very capabilities at the core of these worries. As with many of the problem representations we discuss here, this threat is afforded to other hostile actors, and by other platforms – it is a problem that involves not just TikTok, and not just China.

As many commentators have noted, left out of this problem representation is the extent to which America lacks a strong data protection regulatory framework. But it's also important to recognize the extent to which the motivating concerns, especially as they relate to worries about the ability to use social media platforms to persuade, influence, and coerce, do not depend on access to personal data. Here there is a gap in research and policy – if we what we really care about is something like unfair competition in the marketplace of ideas, and persuasive technology more generally, data protection regulation is not an adequate proxy for this bundle of concerns. To the extent that worries about characteristically cognitive threats are legitimate policy objectives, then the "... greatest risk comes not from what TikTok does, but from what it doesn't do" (Lewis, 2022). Effective influence campaigns can exploit oversights, gaps, and idiosyncrasies in moderation and recommendation systems discovered by exploration and serendipity, rather than direct access to data, and use them effectively without any sort of covert or backchannel access to the platform

An adversary doesn't need to control social media platforms like TikTok to access the sorts of information that are thought to pose risks. "There's so much free-flowing data online that the data ecosystem is essentially unregulated," says Eric Null, co-director of the CDT's Privacy and Data Project. "Foreign governments likely have a pretty trivial time finding information." (Leffer, 2024). Vast troves of data can be purchased from brokers or scraped from the open internet, especially given the advances in AI/ML that afford the capability to mine public data to recover latent information that would otherwise be protected. Political viewpoints can be identified from text corpora (Doan & Gulla, 2022), music playlists can reveal a variety of demographic attributes (Anderson et al., 2021), mental health conditions can be identified from social media data (Xu et al., 2020), and images can be geolocated even when their metadata has been stripped (Haas et al., 2024).

Certainly, the transfer of data to foreign adversary-controlled systems makes such efforts easier, and blocking this a reasonable security objective, but given the range of systems and services that afford the collection and transfer of data about US persons to China, a policy response to this specific problem would need to be articulated in more general terms of data protection and security interest in preventing foreign ownership of critical and sensitive infrastructure. If there is a substantive national security interest in this problem representation, at best the forced divestiture of TikTok is a bandaid. More and more of *who we are* and *what we do* is reflected into data that can be used against us and that can end up in the hands of adversaries.

Finally, if the use of personal data to target political messaging is problematic, this brings other domestic actors into the scope of policy concern. In the context of elections, data-driven campaigns have become the norm, especially in the United States, and the data-holdings of the major American political parties are extensive, and used across a variety of mediums and platforms to target messaging and encourage (and discourage) voting. This is likewise true of corporate actors, including those that offer public relations and reputation management services. While there are well-established norms about the content of political communication, especially during elections, there is much less discussion of the norms around its generation and delivery. If microtargeting is as powerful as its advocates believe it to be, then policy action focussed on TikTok is far too narrow.

Effects produced by this representation of the 'problem'

A primary effect is the framing of what are ultimately a heterogenous range of threats relating to microtargeting, the weaponization of personal data, and opaque processing and deployment for the purposes of influence as a narrow problem involving a platform controlled by a foreign adversary and its access to data. Even setting aside narrow focus on specific state adversaries and considering the broader constellation of actors who have motives and means to engage in manipulative communication of the sort that contributes to cognitive security concerns – policy focussed on cutting off access to some limited category of personal data does not speak directly to the imagined threat.

Tensions around this issue in policy discourse reveal this effect. Should we "... treat U.S. data as a national-security asset, through export controls and other mechanisms" (Dawson & Wheeler, 2022)? Or should we worry that "... none of these harms require data to be transferred. Privacy safeguards will not solve this problem." (Khosla, 2024)

We can also see this effect in a recurring theme in criticism of the TikTok bill - that many of its objectives would be better addressed through improved data protection regulation, modelled after those in the EU. For instance "...[r]ather than handing out arbitrary bans, the US authorities should address the underlying problems of surveillance-based business models by introducing regulations that govern all tech platforms to truly protect our human rights in the digital age" writes the deputy director of Amnesty

International (Armistead, 2024). Concerns about TikTok's data collection tend to blur with advocacy for data protection as an effective policy solution to a broader range of problem representations. It is important to note that this is not likely to be the case. Data protection alone cannot address many of the problem representations we have identified, although a GDPR style regulation in the US could ameliorate some concerns about collection and transfer of data, for instance, an analogue of its Chapter V protections against the transfer of data to states outside the EU that lack adequate data protection laws would prevent data transfer to China.

It should be clear whether policy aims to address concerns about actions of TikTok itself, as an agent of the Chinese government, or the actions it affords to others. The tools and capabilities offered by platforms to advertisers and publishers are available to a multitude of actors, and especially as worries of this sort are often articulated alongside mentions of Cambridge Analytica's infamous use of social media platforms to influence elections (Day, 2019). If we are truly concerned with the ways in which data collection can be used against us as individual and democratic citizens, then the problem may be better described as involving the affordances themselves, and their regulation, oversight, and management, and their basis in widespread surveillance and data hoarding, not specific features of TikTok.

4.3 Cognitive and Epistemic Security

A cluster of concerns related to influence and manipulation in the information environment recur in the policy discourse about the need to ban TikTok because of its risk to national security. These form the basis of the securitizing constructions of the problem representations of TikTok's Chinese ownership, and its collection and processing of data. In section two we described these in relation to an idea in national security literature about cognitive security, and thus we describe this cluster of concerns as involving a conception of cognitive and epistemic security and insecurity. In our data collection we labelled these as:

- Censorship: TikTok can be used to enforce certain limitations on content that American viewers see, perhaps on instruction from the PRC
- Propaganda: TikTok is a vehicle for PRC propaganda and disinformation
- Influence: TikTok enables the PRC to influence perception and opinion, for example, by way of which content is promoted to users by the recommendation system.
- Politically and Socially Dangerous: TikTok is managed and designed in ways that disrupt/disregard norms of political communication (eg affording election interference, disclosing ad funding, affording political voice to foreign agents) or foster social conditions such as polarization, demoralization, and extremism.
- Epistemic pollution: TikTok is designed and managed in ways that foster the spread of misinformation, deep fakes, fake news, and the like.

Presuppositions or assumptions which underpin representation of the 'problem'

Representations of these problems a frequently entangled. A sample from our data collection:

> "Chinese military documents have revealed that the military sees the nature of warfare as "shifting from destroying bodies to paralyzing and controlling the opponent's mind" (Farahany, 2024)
>
> "...the Commission is increasingly disturbed by the role misinformation and disinformation plays in diminishing social cohesion, promoting distrust and division, and undermining principles of equality, respect and human dignity" (Hooton, 2023)
>
> "They are also worried that China could use TikTok's content recommendations to fuel misinformation, a concern that has escalated in the United States during the Israel-Hamas war and the presidential election. Critics say that TikTok has fueled the spread of antisemitism." (Maheshwari & Holpuch, 2024)
>
> "Journalistic deep dives have showcased just how quickly the TikTok algorithm can pinpoint users' moods, beliefs and preferences, leading down a rabbit hole of self-harm and depression. Moreover, the platform's been used to accelerate propaganda against Western governments, becoming one of the main outlets of anti-patriotism and distrust toward democracy." (Lilkov, 2024)
>
> "The United States is also concerned with the PRC's ability to censor information on the Hong Kong protests and other world events to influence U.S. users' views on world events" (Swain, 2020)
>
> "There is evidence that platforms originating in China are pressured to hew to CCP content guidelines—even outside of China's borders, as evidenced by censorship and manipulation on, among others, globally popular Chinese-owned social media platform TikTok" (Kalathil, 2020)
>
> "TikTok also reportedly censors content that the Chinese Communist Party deems politically sensitive, such as content concerning protests in Hong Kong and China's treatment of Uyghurs and other Muslim minorities. This mobile application may also be used for disinformation campaigns that benefit the Chinese Communist Party, such as when TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus" (Executive Order on Addressing the Threat Posed by TikTok, 2020)
>
> "On TikTok, the algorithm tends to show more content from the liberal political spectrum–such as #blacklivesmatter, #woke, or #policereforms–sharpening polarisation and conservative ideas, and is more likely to create eco-chambers than

> open discussion. In Russia's invasion of Ukraine and Israel's war on Gaza, TikTok allowed propaganda narratives to circulate, creating a polarization between the far left and pro-Palestine youth and other voices. Users shared videos, updates, and opinions based on unverified information they found across platforms." (Idris, 2024)

It's important to examine whether this entanglement reflects useful conceptual unities, or whether it stems from genealogies rooted in earlier technological and media contexts, or the political-economic and technological idiosyncrasies of these platforms. It's a potent collection of concerns, but the extent to which they belong together in the problem representations that motivate policy is unclear.

Absent more careful distinctions between these disparate cognitive and epistemic concerns, and the respective conditions and thresholds at which they can be legitimately securitized, there is an assumption that the efforts of adversarial states, like China, to influence foreign audiences on social media platforms like TikTok, are inherently, or are least presumptively, dangerous. This deviates from liberal norms of speech and expression, which often espouse ideals about the positive epistemic function of a media ecosystem with a range of voices, even those which are wrong, offensive, or hostile. The US Supreme court affirmed the constitutional right of Americans to receive even what it deemed to be "communist political propaganda" in Lamont v. Postmaster General, 381 U.S. 301 (1965). Is there a reason why platforms like TikTok that raises the risk, and undermines this right? If so, then there is an assumption that while propaganda itself might not be unduly dangerous, propaganda on TikTok is. There are reasons that could be given to support this idea, but they are not salient in this policy discourse.

Where the term "propaganda" is used, often what is meant is something different, for example, that what misleads is not so much the content of some specific video, but the degree to which it distributed to other users without their expressed preference, or that it bears various signifiers of social acceptance, such as likes, views, comments, etc. The appearance of consensus, salience, and importance is a kind of higher-order information about the content that's distinct from the content itself, but important for understanding its cognitive effect. Complaints about propaganda often mask a more heterogenous and materially grounded set of worries about things like fake accounts, audience segmentation, dark patterns, and misleading affordances.

We see these same kinds of entanglement in concerns about censorship. There is an assumption that because we know that social media platforms make various forms of censorship possible, they may be conducting it in ways we don't know about and that we might disagree with. We know our email systems filter spam, and whether or not we check, we know there's a place we can look to see what has been filtered. This is not true when we want to understand what's in our social media inboxes - our news feeds and homepages, and what could have been there but was omitted.

Policies requiring media platforms to track moderation actions (such as the EU's Digital Services Act of 2022), and which mandate various forms of transparency and viewpoint neutrality (such as Texas House Bill 20 of 2021) express normative ideals about entitlement to be informed when information is censored. However, worries about censorship often presuppose the possibility of an alternative, uncensored, model of these social platforms that might be preferred. This overlooks the scale of information that must be sorted to provide relevant content to a user, and the volume of undesirable content (including illegal content, but also various forms of advertising and spam) that must be filtered for the platform to be usable at all. Problem representations of censorship mixed with concerns about usability, transparency, filtering, and recommendation. In Europe, the Digital Services Act, a significant and influential (Cauffman & Goanta, 2021) policy effort whose objectives include cognitive and epistemic concerns about media platforms, includes a provision requiring media platforms over a certain size to submit all moderation and censoring actions to a public "transparency database". Even just a few months after launch, researchers found it to be overwhelmed by scale and difficult to use for research purposes because of a lack of conceptual consistency around different forms of moderation and types of reasons for action (Trujillo et al., 2023).

That TikTok may have a pronounced risk of radicalizing subsets of its audience relates to worries about epistemic pollution, microtargeting, and the promulgation of conspiracy theories. As with YouTube (Ribeiro et al., 2020), there are risks that optimization for audience engagement can lead to recommendation systems that amplify extremist content and create the conditions which may lead to radicalization (Shin & Jitkajornwanich, 2024a). Moreover, there is always the risk that, once radicalized, an individual may escalate their behaviour to violence. While the function of online polarization, influence and manipulation is not entirely agreed upon in the complex process of radicalization, it is generally accepted that they can amplify the conditions fostering radicalization. Plausible deniability is a feature of cognitive warfare or ‘gray zone conflict’ (Bensahel, 2017) and given the role of TikTok's recommendation and moderation systems in the spread of extremist content (Weimann & Masri, 2023), when the management and control of these is opaque and controlled by a foreign adversary, it is not surprising that concerns about intention arise.

What is left unproblematic in this problem representation

We find these concerns appearing together in various configurations, but it's important to inquire more carefully if they belong together, and why. Policy aiming to resolve worries about propaganda is not obviously related to concerns about censorship - and if there are connections, it may because of some common feature or tendency of the media platform, rather than a useful conceptual grouping.

Related to this, it's not clear that these concepts, with historical roots in very different media, political, and technological contexts, adequately capture the animating concerns. Even if we are persuaded that something about the way that platforms like TikTok offer determined actors opportunities to use them to construct preferences and shape public opinion rises to the level of a security risk, the vocabulary of censorship, propaganda, fake news, disinformation, and the like, have limited value in making the problems tractable for policy action. They are also the subject of substantive scholarly disagreement.

They map poorly to the more specific terminology used by platforms to understand and react to information operations, which "... avoid the umbrella terms most familiar to experts and the public, like "disinformation." [...] and have defined a number of more specific prohibitions—some familiar (like violent threats) and some novel (like "coordinated inauthentic behaviour" or "civic integrity" violations" (Bateman et al., 2021). These vocabularies reflect both platform design and the conceptual framework applied to moderation and trust and safety activities, and there is only limited convergence across platforms. Policy discourse grounded in the concrete material and sociotechnical features of media platforms may avoid conceptual and political baggage that is not only a hinderance to productive political conversation, but that interfaces better with the regulated activities and systems.

Openness and clarity about what is really taking place is especially important in a region of policy and public discourse that is overwhelmed with real and imagined conspiracy - to control, to limit speech, to propagandize and influence, and where the nurturing and protection of various forms of trust, in institutions, experts, and political bodies, is an important precondition to many policy actions.

Effects produced by this representation of the 'problem'

Consider the assumptions that TikTok is a significant site of misinformation and a cause of polarization often appear in policy discourse. TikTok's primary discovery mechanism is a recommendation algorithm that emphasizes inferred and revealed user preferences more so than those of some other platforms that place greater weight on a user's social graph and stated preferences. Evidence about the polarizing effect of social media is mixed (Kubin & Von Sikorski, 2021; Tucker et al., 2018). Worries that TikTok is especially prone to polarization reproduce security concerns specific to TikTok about the possibility of covert and hostile intentions operationalized by the recommendation system, but it is not clear we should suppose any sort of hostile intent is required. Research has found that when optimized to maintain user engagement, as TikTok's algorithm does so effectively, these systems tend to limit counter-attitudinal content and increase polarization (Levy, 2021). The polarizing tendency of social media platforms like TiKTok is also difficult to parse from content published on them, and "...instrumental actors like populists, commercial interests, and partisan media capitalize on social media toward vested ends" (Arora et al., 2022). As a result, policy discourse that links misinformation and polarization to TikTok, it's ownership,

or it's data holdings, misses much of this nuance, and opportunities to better understand underlying public interest in the design and effects of the algorithms that shape our media systems are lost.

A second effect is the embedding of an individualist framing that fits poorly with the policy objects. Terms like censorship and propaganda have long histories and involve direct relationships between determinate speech acts and actors. But when we examine discourse about censorship on social media systems like TikTok, we find a different set of concerns, for instance, about the fairness of systems that arbitrarily reproduce and draw attention to speech acts, and disagreements about how they should work. This implicates important normative questions about the regulation and management of algorithmic power in the democratic media environments, for example, the outsized power of a few "content cartels" (Douek, 2020), that are better approached from the perspective of public interests than individual rights.

If we take a step back and inquire about the origins of national security discourse about epistemic and cognitive security, we can locate this in rapid change and disruption in the technological and politico-economic structure of the media and information environment. It arises because of the perceived novelty and newness of the threat model. But we find that articulations of these cognitive concerns inherits a vocabulary and conceptual apparatus with deep roots in the systems that have been supplanted. At best this confuses efforts to produce policy, and at worse it is actively counterproductive, stoking partisan disagreement about individual rights to speech and freedom from interference that are inadequate to the new phenomena. "Differently from previous efforts targeting human cognition, attitude and opinion-building, which took place under circumstances of information scarcity, cognitive warfare takes places under circumstances of information overabundance" (Bârgăoanu & Durach, 2023 p. 223). Effective policy may require that these older vocabularies be abandoned, and new ones developed to better represent the problems policy should target. One example is (Ördén, 2022) who argues that conceptualizations of cognitive security focused on the individual psychology and behaviour of individuals in media environments "...undermines the agency of the democratic subject", and that instead, securitization should be oriented towards the protection of a more relational conception of political judgement.

5. Conclusion and Future Research

We've examined problem representations found in policy discourse about the US legislative effort to ban TikTok or force its sale to a US owner, that include concerns about cognitive and epistemic insecurity as part of their content.

Two prominent representations are oriented to the fact that TikTok is owned by a company controlled by a hostile foreign adversary, and that TikTok collects a great deal of data, including personal data, that may be made available to an adversary. The hostile control

representation suggests divestiture as a solution, and the data collection representation suggests data protection and privacy regulation. However, the securitizing move from hostile ownership and data collection to security threat depends on underlying concerns about influence, censorship, and manipulation that are not addressed by such policies. While these concerns are peripheral to the actual bill (H.R. 7521), they are entangled with the problem representations and important conceptual ingredients in the claimed threats to security.

Articulations of the problem policy should aim to solve ought to allow us to tease apart what we might find objectionable about teenagers on TikTok approvingly reading bin Laden's letter, from the concerns we might have as to why they are doing it, from specific kinds of insecurity that may be involved. This is particularly important given democratic ideals that strongly discourage regulation of speech environments, and particularly regulation that is articulated in ways that are not viewpoint-neutral. The same is true for worries about political polarization and concerns that public opinion is in some way inauthentically manipulated by way of social media platforms like TikTok.

Echoes of these concerns are found in laws passed in Texas and Florida (Florida Bill 7072 and Texas House Bill 20 respectively). The Florida bill forced social media platforms to provide accounts and publish content for prominent political persons and "journalistic enterprises", and the Texas bill banned social media platforms from moderating content based on political viewpoint. Both bills were vacated on the grounds that they involved unconstitutional compelled speech on the part of the platforms, and that content moderation is protected expression, but a variety of legislative efforts, including challenges to important laws governing social media platforms such as Section 230 of the Communications Decency Act are ongoing.

These efforts are motived in part by concerns that media platforms like TikTok allow their operators to put their finger on the scale to influence the political atmosphere on their platforms and afford direct and indirect opportunities to influence elections and the broader political climate in which policy decisions are made. But this view of the problem assumes that direct interference from platform controllers with specific speech acts is the problem to be solved, a presupposition we also find in policy discourse about the TikTok bill. Removal of the power of platforms to moderate, or to cancel accounts, does little to address ways in which platforms afford and enable influence and interference, or tendencies of some kinds of platform design to induce polarization and misinformation, both of which are phenomena that hostile interference, including that seeking to influence electoral outcomes, seeks to generate.

An assumption common to problem representations about the security threat of TikTok is that the primary mode of hostile action is inorganic, involving forms of coordinated inauthentic behaviour such as bots, artificially boosted content, deliberate de-amplification of dissent, and the like, where data about audiences and content, and direct access to the inner workings of the platform, are used to support a manipulative communication strategy. This way of representing the problem suggests cutting off the means of access as a solution. Consider the

willingness of TikTok to invest almost 2 billion dollars in Project Texas, where TikTok would be entirely housed in American data centres, and directly overseen by the Committee on Foreign Investment in the United States (CFIUS). It may be that ByteDance simply wishes to continue to do business in America. But given the extent to which is it is, or may be, controlled by the PRC, we might also think that this suggests that organic influence is just as important - that a platform where large audiences can rapidly and virally be developed and engaged is itself the primary object of strategic value. When we consider the information operations and electoral influence campaigns that have been conducted successfully on US controlled platforms, and the extent to which this form of media appears to be prone to misinformation, polarization, radicalization and extremism (Shin & Jitkajornwanich, 2024b) an adversary might reasonably assess that the continued prominence of this form of media is desirable, and regulation which substantively changes the way it works worth forestalling.

This brings us back to the point we most wish to emphasize - if there are important and legitimate cognitive and epistemic security concerns about TikTok, the policy and motivating problem representations do not address them clearly. These affect other platforms aside from TikTok, regardless of ownership. They carry with them conceptual baggage that is a poor fit with the actual mechanisms involved and the theoretical and material basis on which platforms detect, monitor and react to these threats. We are far from the first to argue for conceptual clarity as a necessary basis for strong policy. Indeed, Andrew Futter argued in this journal for retirement of the word ‘cyber’ from the security studies context citing concern that the lack of consensus about the term could lead to "misunderstanding and bad policy" (Futter, 2018 p. 201). In the current case, we are less concerned about eliminating a term than we are with clarifying scope: What do policy makers mean, and what does the public understand, when they talk about manipulative techniques, when they mention risks of censorship, biased moderation, and dangerous recommendation algorithms? What are we protecting against, and how best can we enact that protection?

The most important task for future research is connective. There is relevant work in social and cognitive psychology exploring individual susceptibility to manipulative communication, in algorithm and interface design finding methods to impede polarization and reduce the spread of mis/disinformation, in the ethics of manipulation and nudging on tensions between ideals of autonomy and engineered information infrastructure, and in political science, communication theory and law on our understanding of information transmission, the role of media institutions, and strategies to address gaps where media regulation and governance has lagged sociotechnical change. We worry that the full range of relevant interdisciplinary knowledge is underrepresented within the narrow confines of policy in the security context. This is especially important given the extent to which securitization places some of this policymaking and enactment behind closed doors. Even the pursuit of narrow objectives, such as the prevention of election interference, efforts to protect the information environment bring into scope a huge range of our ordinary behaviour (Mellamphy, 2023; Rini, 2021).

In the absence of conceptual, but also technical clarity, about the category of cognitive and epistemic risks, a range of policy tensions and lacunae emerge. The TikTok bill depends in its implementation on fact that TikTok is predominantly delivered by an app, and not over the web, and that access to apps happens to be controlled by a duopoly of American corporations (Google and Apple). A ban would be implemented by forcing these to remove the app from their American app stores. Given the extent to which outsized corporate power to influence the media environment appears in problem representations about the threat of TikTok, there's an obvious tension when the solution depends on just this kind of power, but wielded by different actors. This is important when we try to better understand the normative content of concerns about propaganda, censorship, and influence, which often involve ideals about intellectual and political autonomy that sit uncomfortably alongside the reality of highly centralized and private governance (Messina, 2023) of much of the information environment.

There is a risk, not only of having policy that doesn't work, and exhausting limited resources and political will, but of engaging in counter-productive policy, which undermines rather than restores trust in media and political institutions, that increases polarization, or that incidentally enacts forms of authoritarianism it aimed to resist. A major challenge for policy response to cognitive and epistemic insecurity is finding ways to intermediate experts, platforms, civil society and political representatives in ways that are effective but also consistent with democratic norms and ideals about the ethical and epistemic value of free and open media environments.

References

15 CFR 791.4, Code of Federal Regulations (2024). https://www.ecfr.gov/current/title-15/part-791/section-791.4#p-791.4(a)

Aho, B. (2023). Toward an Algorithmically Planned Economy: Data Policy and the Digital Restructuring of China. In *China's Digital Civilization* (pp. 40–55). Routledge.

Anderson, I., Gil, S., Gibson, C., Wolf, S., Shapiro, W., Semerci, O., & Greenberg, D. M. (2021). "Just the way you are": Linking music listening on Spotify and personality. *Social Psychological and Personality Science*, *12*(4), 561–572.

Anja Karadeglija. (2022). Canada "closely monitoring" U.S. bill to ban TikTok, government says. *National Post (f/k/a The Financial Post) (Canada)*.

Armistead, L. (2024, April 25). *US: TikTok ban won't solve harms of Big Tech's invasive surveillance*. https://www.amnesty.org/en/latest/news/2024/04/us-tiktok-ban-wont-solve-harms-of-big-techs-invasive-surveillance/

Arora, S. D., Singh, G. P., Chakraborty, A., & Maity, M. (2022). Polarization and social media: A systematic review and research agenda. *Technological Forecasting and Social Change*, *183*, 121942. https://doi.org/10.1016/j.techfore.2022.121942

Bacchi, C. (2009). *Analysing policy*. Pearson Higher Education AU.

Bacchi, C. (2012). Why Study Problematizations? Making Politics Visible. *Open Journal of Political Science*, *02*(01), 1–8. https://doi.org/10.4236/ojps.2012.21001

Bacchi, C., Goodwin, S., Bacchi, C., & Goodwin, S. (2016). Making politics visible: The WPR approach. *Poststructural Policy Analysis: A Guide to Practice*, 13–26.

Baker-White, E. (2024, July 2). Lawmakers' Angry Statements About TikTok Could Hamstring Their Ban. *Forbes*. https://www.forbes.com/sites/emilybaker-white/2024/03/28/lawmakers-statements-on-tiktok-may-hamstring-their-ban/

Balzacq, T. (2009). Constructivism and securitization studies. In *The Routledge handbook of security studies* (pp. 72–88). Routledge.

Bârgăoanu, A., & Durach, F. (2023). Cognitive Warfare: Understanding the Threat. In *Routledge Handbook of Disinformation and National Security* (pp. 221–236). Routledge.

Barocas, S. (2012). The price of precision: Voter microtargeting and its potential harms to the democratic process. *Proceedings of the First Edition Workshop on Politics, Elections and Data*, 31–36.

Basch, C. H., Meleo-Erwin, Z., Fera, J., Jaime, C., & Basch, C. E. (2021). A global pandemic in the time of viral memes: COVID-19 vaccine misinformation and disinformation on

TikTok. *Human Vaccines & Immunotherapeutics*, *17*(8), 2373–2377. https://doi.org/10.1080/21645515.2021.1894896

Bateman, J., Thompson, N., & Smith, V. (2021). How social media platforms' community standards address influence operations. *CEIP: Carnegie Endowment for International Peace*.

Bensahel, N. (2017). Darker Shades of Gray: Why Gray Zone Conflicts Will Become More Frequent and Complex. *Foreign Policy Research Institute*, *13*.

Bond, S. (2024, August 23). Meta takes down more accounts tied to Iranian hackers targeting the U.S. election. *NPR*. https://www.npr.org/2024/08/23/g-s1-19350/meta-iran-hacking-election-trump-harris-biden

Brar, A. (2023, October 23). Iran Joins Middle East Propaganda War on China's TikTok. *Newsweek*. https://www.newsweek.com/china-iran-propaganda-douyin-social-media-antisemitic-1836806

Buzan, B., & Wæver, O. (1997). Slippery? Contradictory? Sociologically untenable? The Copenhagen school replies. *Review of International Studies*, *23*(2), 241–250.

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cauffman, C., & Goanta, C. (2021). A new order: The digital services act and consumer protection. *European Journal of Risk Regulation*, *12*(4), 758–774.

Ceci, L. (2024, February 2). *Most watched TikTok video worldwide as of July 2023*. https://www.statista.com/statistics/1448441/top-tiktok-videos-views/

Chayka, K. (2022, March 3). Watching the World's "First TikTok War." *The New Yorker*. https://www.newyorker.com/culture/infinite-scroll/watching-the-worlds-first-tiktok-war

Claverie, B., & Du Cluzel, F. (2022). *"Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare*. NATO Collaboration Support Office.

Collines, L. (2018, July 26). Russia Gives Lessons in Electronic Warfare. *Association of the US Army*. https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare

Cox, R. W. (1981). Social forces, states and world orders: Beyond international relations theory. *Millennium*, *10*(2), 126–155.

Dawson, J., & Wheeler, T. (2022). How to tackle the data collection behind Chinas AI ambitions. *Brookings Institute*. https://www.brookings.edu/articles/how-to-tackle-the-data-collection-behind-chinas-ai-ambitions/

Day, P. (2019). Cambridge Analytica and Voter Privacy. *Geo. L. Tech. Rev.*, *4*, 583.

De Campos, T. C. (2020). The Traditional Definition of Pandemics, Its Moral Conflations, and Its Practical Implications: A Defense of Conceptual Clarity in Global Health Laws and Policies. *Cambridge Quarterly of Healthcare Ethics*, *29*(2), 205–217. https://doi.org/10.1017/S0963180119001002

Doan, T. M., & Gulla, J. A. (2022). A Survey on Political Viewpoints Identification. *Online Social Networks and Media*, *30*, 100208. https://doi.org/10.1016/j.osnem.2022.100208

Dostri, O. (2024). Israel's Struggle with the Information Dimension and Influence Operations during the Gaza War. *MILITARY REVIEW*, *1*.

Douek, E. (2020). The rise of content cartels. *Knight First Amendment Institute at Columbia*.

Evans, J. (2022). War in the Age of TikTok. *Russian Analytical Digest*, *280*, 17–19.

Executive Order on Addressing the Threat Posed by TikTok (2020). https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

Farahany, Ni. (2024, March 25). TikTok is part of China's cognitive warfare campaign. *The Guardian*. https://www.theguardian.com/commentisfree/2023/mar/25/tiktok-china-cognitive-warfare-us-ban

Fung, B. (2023, March 21). Lawmakers say TikTok is a national security threat, but evidence remains unclear. *CNN*. https://www.cnn.com/2023/03/21/tech/tiktok-national-security-concerns/index.html

Futter, A. (2018). 'Cyber'semantics: Why we should retire the latest buzzword in security studies. *Journal of Cyber Policy*, *3*(2), 201–216.

Gehl, R. W., & Lawson, S. (2024). Automated Masspersonal Social Engineering. *The De Gruyter Handbook of Robots in Society and Culture*, *3*, 119.

Gursky, J., Riedl, M. J., Joseff, K., & Woolley, S. (2022). Chat apps and cascade logic: A multi-platform perspective on India, Mexico, and the United States. *Social Media+ Society*, *8*(2), 20563051221094773.

Haas, L., Skreta, M., Alberti, S., & Finn, C. (2024). Pigeon: Predicting image geolocations. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 12893–12902.

Helberg, J. (2023, November 20). Why TikTok is a National Security Threat. *The National Interest*. https://nationalinterest.org/blog/techland/why-tiktok-national-security-threat-207369

Hersch, W., Mclain, M., & others. (2024). Inside the Gates: Cultivating Cognitive Security to Defend the Homeland. *Journal of Indo-Pacific Affairs*, *7*(4).

Hersh, E. D. (2015). *Hacking the electorate: How campaigns perceive voters*. Cambridge University Press.

Hooton, P. (2023). *Inquiry into the risk posed to Australia's democracy by Foreign Interference Through Social*.

Hung, T.-C., & Hung, T.-W. (2022). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. *Journal of Global Security Studies*, *7*(4). https://doi.org/10.1093/jogss/ogac016

Idris, I. (2024, August 8). Deceptive Trends: The Societal Impact of Disinformation on TikTok. *Australian Institute of International Affairs*. https://www.internationalaffairs.org.au/australianoutlook/deceptive-trends-the-societal-impact-of-disinformation-on-tiktok/

Kalathil, S. (2020). The Evolution of Authoritarian Digital Influence: Grappling with the New Normal. *Prism*, *9*(1), 32–51.

Kefford, G., Dommett, K., Baldwin-Philippi, J., Bannerman, S., Dobber, T., Kruschinski, S., Kruikemeier, S., & Rzepecki, E. (2023). Data-driven campaigning and democratic disruption: Evidence from six advanced democracies. *Party Politics*, *29*(3), 448–462. https://doi.org/10.1177/13540688221084039

Khosla, V. (2024, April 9). The US is right to target TikTok. *Financial Times*. https://www.ft.com/content/69caf324-2ac0-4b53-a0b4-1f2ecae6e29e

Knockel, J., Kato, K., & Dirks, E. (2023). *Missing Links: A comparison of search censorship in China*.

Köckritz, A. (2023). *In a Savvy Disinformation Offensive, China Takes Aim at Taiwan Elections*. Mercator Institute for China Studies.

Kubin, E., & Von Sikorski, C. (2021). The role of (social) media in political polarization: A systematic review. *Annals of the International Communication Association*, *45*(3), 188–206.

Kubrin, C. E. (2008). Making order of disorder: A call for conceptual clarity. *Criminology & Pub. Pol'y*, *7*, 203.

Lakomy, M. (2024). In Mapping Digital Jihad. *Perspectives on Terrorism*, *18*(2), 82–99.

LaMattina, L. (2024, March 24). Taiwan labels TikTok as national security threat. *Taiwan News*. https://www.taiwannews.com.tw/news/5121862

Lavoy, N. (2024, August 14). TikTok Is a Threat to National Security, but Not for the Reason You Think. *RAND*. https://www.rand.org/pubs/commentary/2024/08/tiktok-is-a-threat-to-national-security-but-not-for.html

Leffer, L. (2024, March 22). Banning TikTok Would Do Basically Nothing to Protect Your Data. *Scientific American*. https://www.scientificamerican.com/article/tiktok-ban-data-privacy-security/

Levy, R. (2021). Social media, news consumption, and polarization: Evidence from a field experiment. *American Economic Review*, *111*(3), 831–870.

Lewis, J. A. (2022, November 14). TikTok and the First Amendment. *Center for Strategic and International Studies*. https://www.csis.org/analysis/tiktok-and-first-amendment

Lilkov, D. (2024, April 17). Time to ban TikTok in the EU. *Politico*. https://www.politico.eu/article/tiktok-ban-eu-china-social-media-apps/

Maheshwari, S., & Holpuch, A. (2024, January 20). Why the U.S. Is Forcing TikTok to Be Sold or Banned. *The New York Times*. https://www.nytimes.com/article/tiktok-ban.html

Martina, M., & Shepardson, D. (2023, August 16). Close to half of American adults favor TikTok ban, Reuters/Ipsos poll shows. *Reuters*. https://www.reuters.com/technology/close-half-americans-favor-tiktok-ban-reutersipsos-poll-2023-08-16/

McBride, M. K., Gold, Z., & Stricklin, K. (2020). Social Media Bots: Implications for Special Operations Forces. *Center for Naval Analysis, September*.

McKay, S., & Tenove, C. (2020). Disinformation as a Threat to Deliberative Democracy. *Political Research Quarterly*, 106591292093814. https://doi.org/10.1177/1065912920938143

Mellamphy, N. B. (2023). The Fog of Peace: War on Terror, Surveillance States, and Post-human Governance. *Washington University Review of Philosophy*, *3*, 63–82.

Messina, J. (2023). *Private censorship*. Oxford University Press.

Milmo, D., & Davidson, H. (2022, November 28). Chinese bots flood Twitter in attempt to obscure Covid protests. *The Guardian*. https://www.theguardian.com/technology/2022/nov/28/chinese-bots-flood-twitter-in-attempt-to-obscure-covid-protests

Morell, M. J. (2016, December 11). Fmr. CIA Acting Dir. Michael Morell: "This Is the Political Equivalent of 9/11." *The Cipher Brief*. https://www.thecipherbrief.com/article/exclusive/fmr-cia-acting-dir-michael-morell-political-equivalent-911-1091#.WE6RWJk6AUU.twitter

Office of the Secretary of Defense. (2023). *Military and Security Developments Involving the People's Republic of China* [Annual Report to Congress]. https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF

Ördén, H. (2022). Securitizing cyberspace: Protecting political judgment. *Journal of International Political Theory*, *18*(3), 375–392.

Paul, C., & Matthews, M. (2016). *The Russian Firehose of Falsehood Propaganda Model: Why It Might Work and Options to Counter It*. RAND Corporation. https://doi.org/10.7249/PE198

Paul, K. (2024, September 17). Meta bans Russian state media for “foreign interference.” *Reuters*. https://www.reuters.com/business/media-telecom/meta-bans-rt-other-russian-state-media-networks-2024-09-17/

Protecting Americans from Foreign Adversary Controlled Applications Act. (2024). https://www.congress.gov/bill/118th-congress/house-bill/7521

Public Safety Canada. (2023). *Security Concerns with TikTok Social Media Application*. Public Safety Canada. https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240614/22-en.aspx?wbdisable=true

Reuters. (2022, December 23). TikTok admits using its app to spy on reporters in effort to track leaks. *The Guardian*. https://www.theguardian.com/technology/2022/dec/22/tiktok-bytedance-workers-fired-data-access-journalists#:~:text=TikTok%20has%20admitted%20that%20it,according%20to%20an%20internal%20email.&text=The%20data%20was%20accessed%20by,track%20the%20reporters'%20physical%20movements

Ribeiro, M. H., Ottoni, R., West, R., Almeida, V. A., & Meira Jr, W. (2020). Auditing radicalization pathways on YouTube. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 131–141.

Rini, R. (2021). Weaponized skepticism. *Political Epistemology*, *31*.

Roemmele, A., & Gibson, R. (2020). Scientific and subversive: The two faces of the fourth era of political campaigning. *New Media & Society*, *22*(4), 595–610.

Rogers, Z. (2021). The Promise of Strategic Gain in the Digital Information Age. *The Cyber Defense Review*, *6*(1), 81–106.

Sang, T. H., Thien, T. T., & Nhi, L. T. Y. (2024, June 20). How Taiwan fights the disinformation war. *The Lowy Institute*. https://www.lowyinstitute.org/the-interpreter/how-taiwan-fights-disinformation-war

Shin, D., & Jitkajornwanich, K. (2024a). How Algorithms Promote Self-Radicalization: Audit of TikTok's Algorithm Using a Reverse Engineering Method. *Social Science Computer Review*, *42*(4), 1020–1040. https://doi.org/10.1177/08944393231225547

Shin, D., & Jitkajornwanich, K. (2024b). How Algorithms Promote Self-Radicalization: Audit of TikTok's Algorithm Using a Reverse Engineering Method. *Social Science Computer Review*, *42*(4), 1020–1040. https://doi.org/10.1177/08944393231225547

Southwick, L., Guntuku, S. C., Klinger, E. V., Seltzer, E., McCalpin, H. J., & Merchant, R. M. (2021). Characterizing COVID-19 content posted to TikTok: Public sentiment and response during the first phase of the COVID-19 pandemic. *Journal of Adolescent Health*, *69*(2), 234–241.

Swain, J. (2020). Can the US Government Sanction TikTok Like It Is Iran's Nuclear Program? *Boston College Intellectual Property and Technology Forum*, *2020*, 1–13.

Tappin, B. M., Wittenberg, C., Hewitt, L. B., Berinsky, A. J., & Rand, D. G. (2023). Quantifying the potential persuasive returns to political microtargeting. *Proceedings of the National Academy of Sciences*, *120*(25), e2216261120. https://doi.org/10.1073/pnas.2216261120

Trujillo, A., Fagni, T., & Cresci, S. (2023). The DSA Transparency Database: Auditing self-reported moderation actions by social media. *arXiv Preprint arXiv:2312.10269*.

Tucker, J., Guess, A., Barbera, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3144139

Waltzman, R. (2017). *The Weaponization of Information: The Need for Cognitive Security*. Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity on April 27, 2017. https://www.armed-services.senate.gov/imo/media/doc/Waltzman_04-27-17.pdf

Weimann, G., & Masri, N. (2023). Research Note: Spreading Hate on TikTok. *Studies in Conflict & Terrorism*, *46*(5), 752–765. https://doi.org/10.1080/1057610X.2020.1780027

Weimann, G., & Weimann-Saks, D. (2024). Coping with Hamas's Psychological Warfare during the Gaza War. *Studies in Conflict & Terrorism*, 1–20. https://doi.org/10.1080/1057610X.2024.2327669

Woolley, S. (2023). *Manufacturing consensus: Understanding propaganda in the era of automation and anonymity*. Yale University Press.

Wray, C. (2022, December 2). *2022 Josh Rosenthal Memorial talk*. https://fordschool.umich.edu/video/2022/christopher-wray-2022-josh-rosenthal-memorial-talk

Wu, S. (2024, March 8). Biden Backs Effort to Force Sale of TikTok by Chinese Owners. *Wall Street Journal*. https://www.wsj.com/politics/policy/biden-backs-effort-to-force-sale-of-tiktok-by-chinese-owners-ba989656

Xu, Z., Pérez-Rosas, V., & Mihalcea, R. (2020). Inferring social media users' mental health status from multimodal information. *Proceedings of the Twelfth Language Resources and Evaluation Conference*, 6292–6299.

Yang, P., & Tang, L. (2018). "Positive Energy": Hegemonic intervention and online media discourse in China's Xi Jinping Era. *China: An International Journal*, *16*(1), 1–22.