Selected Papers of #AoIR2022:
The 23rd Annual Conference of the
Association of Internet Researchers
Dublin, Ireland / 2-5 Nov 2022

SHAPING APP DATA PUBLICS AS A NATIONAL SECURITY ISSUE: A COMPARATIVE ANALYSIS OF THE CFIUS-GRINDR AND CFIUS-TIKTOK RULINGS

David Myles
Institut national de la recherche scientifique

CFIUS and the US Interest in Platform Data Practices

Charged with evaluating the implications that large business transactions pose for US national security, the Committee on Foreign Investment in the United States (CFIUS) has been at the centre of two major controversies in 2019. In March, CFIUS labelled the queer dating app Grindr as a risk for national security and forced the Chinese conglomerate Kunlun Tech, which had taken control of the app a year prior, to divest from it by June 2020 (Myles, accepted). In November, the Committee launched an investigation into the Chinese company ByteDance, owner of the popular app TikTok, after it acquired the app Musical.ly in 2017 (Gray, 2021). These investigations came in the wake of the new Foreign Investment Risk Review Modernization Act (FIRRMA, 2018), which extended CFIUS's scope to oversee business transactions pertaining to digital platforms that collect or monetize the sensitive data of US citizens. Once predominantly concerned with military and energy asset acquisitions, the new FIRRMA-empowered CFIUS shifted its focus to digital platforms and their data infrastructures to ensure that their foreign acquisition would not hinder the United States' national security and technological superiority. This shift transformed CFIUS into an influential actor in matters of Internet regulation and platform data (mal)practice.

The objective of this paper is to compare *how* TikTok and Grindr, then both Chinese-owned apps, were construed as threats to US national security. Specifically, it highlights how app data publics are increasingly at the heart of important discursive struggles that seek to determine whether or how they constitute a risk. As our analysis shows, these discursive struggles have been exacerbated by the ongoing US-China trade conflict that opposes the two nationalist superpowers in a race to control key digital assets (Kokas, 2018).

Myles, D. (2022, November). *Shaping App Data Publics as a National Security Issue: A Comparative Analysis of the CFIUS-Grindr and CFIUS-TikTok Rulings*. Paper presented at AoIR 2022: The 23rd Annual Conference of the Association of Internet Researchers. Dublin, Ireland: AoIR. Retrieved from http://spir.aoir.org.

Shaping Data Publics as a Contentious National Security Issue

This paper mobilizes a political approach to communication to discuss the implications that the datafication of our daily and intimate lives by social media apps raise in terms of Internet regulatory issues (Wilken et al., 2019). Specifically, it highlights how apps build new 'data publics' (Mörtenböck & Mooshammer, 2020), that is, how datafication increasingly participates in "defining the modalities through which social groups are constituted and recognized as such, and in shaping the legitimacy of the sociopolitical claims that can be made in their name or against them" (Myles, accepted: 5). It also considers how LGBTQ+ dating apps increasingly manage sensitive queer data (Lutz & Rancini, 2017), like HIV status, gender identity, and sexual orientation, which gives way to new queer data publics that can be weaponized for political and socioeconomic gains.

To do so, this paper critically examines how the CFIUS-Grindr and the CFIUS-TikTok rulings have each been distinctly shaped *as* public controversies by a series of stakeholders (e.g., journalists, pundits, politicians, platform owners, legal experts). To do so, we turn to controversy analysis, which is useful to understand how stakeholders collectively delineate, often through discursive struggles, the regulatory frames that should govern digital platforms and, thus, participate in the social and material construction of technologies (Epstein et al., 2016).

To conduct our comparative controversy analysis, we used the Google News search engine to collect 294 papers pertaining to the CFIUS-TikTok ruling and 107 papers pertaining to the CFIUS-Grindr rulings. While using Google's search engine presents inherent methodological limitations relating to the platform's algorithmic opacity and biases, this strategy still enabled us to observe emerging trends and identify key stakeholders. Our analysis was informed by additional documentation, like IPO filings and shareholders' reports, CFIUS documentation, and legal reports produced by specialized trade law firms. The selected articles were coded in the qualitative software QDA Miner and were the object of an STS-informed discourse analysis focused on the authoritative – and often contested – claims through which Internet regulatory issues are publicly shaped (Epstein et al., 2016).

The Unequal Treatment of Grindr's and TikTok's Data Publics

Our analysis highlights how the CFIUS-Grindr and the CFIUS-TikTok rulings similarly sought to construe the Chinese ownership of social media apps as a potential threat to US national security by overtly conjuring anti-Chinese sentiment. Namely, CFIUS posited that significant risks were associated with having sensitive data infrastructures fall 'into the wrong hands' or seeing the personal data of US citizens 'intercepted' by Chinese authorities. However, a closer examination revealed that TikTok's and Grindr's

data publics were, in fact, made to matter quite differently by key stakeholders, like US officials and pundits.

On the one hand, the acquisition of Musical.ly by Bytedance was predominantly framed as a data privacy matter. As stated by former White House Press Secretary Kayleigh McEnany, apps like TikTok "collect significant amounts of private data on users", and the Trump administration is "committed to protecting the American people from all cyber threats" (Associated Press, 2020). On the other hand, the CFIUS investigation into Grindr's corporate data practices was mainly made to matter by depicting LGBTQ+ citizens as higher security risks for the United States because of their sexual and gender identities. This was accomplished by construing Grindr users as being more vulnerable to covert blackmail initiatives that could result in key US citizens disclosing sensitive information to the Chinese authorities.

As such, the CFIUS-TikTok ruling was mainly portrayed as a privacy and human rights issue while the Grindr ruling seldom was. And while the CFIUS-Grindr ruling was made to matter by questioning the allegiance of Grindr's queer users (e.g., by positing their potential 'political disenfranchisement'), the allegiance of TikTokers was never challenged in the same way, thus hinting at the unequal treatment that LGBTQ+ citizens face in matters of data privacy and national security. This paper concludes by raising some of the implications that datafication poses for the LGBTQ+ communities, as they have little control over the regulatory frames that oversee their activities online (DeNardis & Hackl, 2016).

References

Associated Press (2020) Trump orders Chinese owner of TikTok to sell U.S. assets. *CTV News*, 14 August.

DeNardis L and Hackl AM (2016) Internet control points as LGBT rights mediation. *Information, Communication & Society* 19(6): 753-770.

Epstein D, Katzenbach C and Musiani F (2016) Doing internet governance: practices, controversies, infrastructures, and institutions. *Internet Policy Review* 5(3): 1-14.

FIRRMA (2018) "TITLE XVII—REVIEW OF FOREIGN INVESTMENT AND EXPORT CONTROLS". U.S. Department of the Treasury, United States.

Gray J (2021) The geopolitics of 'platforms': the TikTok challenge. *Internet Policy Review* 10(2).

Kokas A (2018) Platform Patrol: China, the United States, and the Global Battle for Data Security. *The Journal of Asian Studies* 77(4): 923-933.

Lutz C and Ranzini G (2017) Where dating meets data: Investigating social and institutional privacy concerns on Tinder. *Social Media+ Society* 3(1): 1-12.

Mörtenböck P and Mooshammer H (2020) Introduction. In: Mörtenböck P and Mooshammer H (eds) *Data Publics: Public Plurality in an Era of Data Determinacy*. London: Routledge, pp. 1-25.

Myles D (accepted) Grindr? It's a 'Blackmailer's Goldmine'! The Weaponization of Queer Data Publics amid the US-China Trade Conflict. *Sexualities*, *Special Issue on Sexual Datafication.*

Wilken R, Burgess J and Albury K (2019) Dating apps and data markets: A political economy of communication approach. *Computational Culture* 7: 1-26.