Bernot, Ausma; Cooney-O'Donoghue, Diarmuid; Mann, Monique

Article

Governing Chinese technologies: TikTok, foreign interference, and technological sovereignty

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Bernot, Ausma; Cooney-O'Donoghue, Diarmuid; Mann, Monique (2024) : Governing Chinese technologies: TikTok, foreign interference, and technological sovereignty, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 13, Iss. 1, pp. 1-26, https://doi.org/10.14763/2024.1.1741

This Version is available at:
https://hdl.handle.net/10419/285316

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 13 **Issue** 1

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Governing Chinese technologies: TikTok, foreign interference, and technological sovereignty

Ausma Bernot *Griffith University* a.bernot@griffith.edu.au
Diarmuid Cooney-O'Donoghue *University of Warwick*
Monique Mann *Victoria University of Wellington*

DOI: https://doi.org/10.14763/2024.1.1741

Published: 27 February 2024
Received: 31 July 2023 **Accepted:** 1 December 2023

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Bernot, A. & Cooney-O'Donoghue, D. & Mann, M. (2024). Governing Chinese technologies: TikTok, foreign interference, and technological sovereignty. *Internet Policy Review*, *13*(1). https://doi.org/10.14763/2024.1.1741

Keywords: TikTok, Foreign interference, Digital sovereignty, Geopolitics, Surveillance

Abstract: TikTok bans have been presented as one solution to threats to national security, data security, foreign interference, child safety, and foreign espionage. In this article we investigate four countries/regions — Australia, the United Kingdom, the United States, and the European Union — that have banned or attempted to govern TikTok, examining the policy and legal bases for such restrictions. Our analysis is conceptually informed by legal and political narrations of foreign interference and technological sovereignty. We approach this with particular attention to countries with existing intelligence and data sharing agreements (i.e. three members of the Five Eyes alliance and the trilateral AUKUS alliance) and the European Union given its regulatory approach to data protection. This research makes significant and timely contributions to the geopolitics of TikTok and foreign interference in an international context. It informs inconsistencies in regulatory and legal approaches relating to foreign interference and data sovereignty, beyond "China threat" narratives. We argue that the European Union regulation presents an approach that attempts to protect citizens and citizen data rather than attack platforms and governments that challenge Western technological hegemony.

1 Introduction

The Chinese social media app TikTok has rapidly grown in popularity to become one of the leading social media platforms globally, especially among young users. This popularity has been met with increasing scrutiny from nations such as the United States (US), United Kingdom (UK), Australia, and in the European Union (EU) due to concerns of individual privacy, foreign interference, and cyber security. Most of these concerns stem from TikTok's relationship with the Chinese Communist Party (CCP) and TikTok's corporate links to the China-based ByteDance via their Cayman Islands-based parent company. These concerns reached a critical point in August 2020 when the Trump administration issued a divestiture order to TikTok, and the company began searching for US buyers. Subsequently, in March 2023 TikTok CEO Shou Zi Chew appeared in front of the US House Energy and Commerce Committee, where he met intense questioning from US Members of Congress (Clayton, 2023).

This Committee hearing followed concerns about the risks of TikTok, leading to a ban on US federal government employees from having TikTok on their work devices in December 2022 (Ingram, 2022). Likewise, in March 2023, the EU implemented a ban on government devices (McCallum, 2023), as did the UK in March 2023 (Sabbagh, 2023) and Australia in April 2023 (Dreyfus, 2023). A series of other countries followed suit, including the other two Five Eyes countries New Zealand (Neilson, 2023) and Canada (Treasury Board of Canada Secretariat, 2023), as well as several others, like India, that banned the app altogether (Kumar & Thussu, 2023). Since the 1980s, global technological engagement with China, and in turn the Chinese Communist Party (CCP), has grown, propelling the nation to the forefront of the international economic landscape despite well documented human rights concerns. China has become a global technology power, with Chinese technology companies leading the way in new technology developments such as 5G, Artificial Intelligence (AI), and electric batteries (Gaida et al., 2023). China's significant technology advancements have challenged the dominance of Western (and mostly US) technology firms (see Gray, 2021). The US, Australia, and China have engaged in retaliatory measures, imposing tariffs, export controls, and investment restrictions (Roberts & Lamp, 2021). In this article, we focus on the US, Australia, the UK, and the EU that provide a rich geopolitical cross-section to compare and contrast national (and regional) approaches to TikTok adoption as an example of a popular Chinese technology. We focus on these jurisdictions as they share strategic interests and are engaged in various intelligence and security alliances. Moreover, the rise of Chinese technology is challenging Western, especially US, hegemony in

social media and digital platforms with geopolitical consequences (Gray, 2021). We also selected the US, UK, Australia, and the EU for examination given that each has introduced varying measures to counter and/or regulate TikTok within their respective jurisdictions, the nuances of which have been made public through policy documents and statements made to the media by political representatives.

There is a longer history of geopolitical tensions to consider that extends beyond the social media platform of TikTok to other Chinese technologies. For example, over twenty countries globally, including Australia and the US, have banned the use of Huawei 5G technology due to security and privacy concerns (Roberts & Lamp, 2021). Likewise, in Australia, Chinese-made technologies have featured in concerns over national security and foreign interference, including Australian government audits into Chinese-made CCTV surveillance cameras installed in government buildings and drones (Bernot & Walsh, 2023). Australian politicians and the Australian Security Intelligence Organisation (ASIO) have raised concerns that China-made cameras pose foreign interference, espionage, and national security risks (Belot, 2023), leading to the removal of these cameras from government offices (Bagshaw, 2023).

There is limited literature that examines the geopolitical dimensions to responses to TikTok comparatively (see Gray, 2021) and specifically across the domains of foreign interference and technological and digital sovereignty. This article addresses this imbalance by examining how the US, Australia, the UK, and the EU have responded to TikTok in each respective jurisdiction. These country-(and regional) level case studies reveal high-profile investigations into foreign interference threats and formal responses to manage the perceived risks of TikTok (Table 1). While the US, Australia, and the UK are in close geopolitical coalition under the auspices of the trilateral AUKUS alliance and the wider Five Eyes intelligence alliance (in addition to New Zealand and Canada), the EU has world-leading data protection regulation, the Digital Services Act (DSA) that aims to regulate Very Large Online Platforms (VLOPs) and search engines (VLOSEs) (European Commission, 2023a), and at the time of writing is introducing new measures to regulate Artificial Intelligence (i.e. the EU AI Act). The EU also has taken a strong stance on issues of technological sovereignty (and against the US) and is included to provide further comparative perspectives outside the AUKUS alliance. The EU rights-based approach is an interesting comparator given its protectionist and rights based approaches to safeguarding citizen data.

2 Aims and approach

We examine responses to TikTok in the US, UK, Australia, and the EU through the conceptual lenses of technological sovereignty and foreign interference, through analysis of relevant law, policy, and public statements made by officials, to document and understand responses to Chinese technologies, specifically TikTok, as a leading Chinese social media platform. The article proceeds across four steps. First, we examine TikTok and its corporate structures, and connections with the CCP. Second, we introduce the framing of foreign interference and technological sovereignty. Third, we examine jurisdictional responses to TikTok considering their policies and positions in relation to foreign interference and technological sovereignty. Fourth, and finally, we discuss the implications of these findings and consider how foreign interference and technological sovereignty inform the governance of TikTok, and in turn what this may mean for global internet governance as applied to Very Large Online Platforms (VLOPs).

2.1 TikTok: corporate structure, data security, and political influence

Chinese companies that internationalise often face dual pressure to comply with Chinese regulations domestically and national data protection scrutiny in other countries (Jia & Ruan, 2020). However, the growth of Chinese companies internationally is often linked with national security risks that can also mask national economic interests, especially when they challenge US hegemony with geopolitical consequences (Bernot, 2022; Gray, 2021). The surveillance capabilities of Chinese technologies and service providers have contributed to the complexity of this dynamic. This is because data and cyber security is significant from a geopolitical perspective (Gray, 2021) and, as we argue in this paper, is closely connected to notions of technological sovereignty and foreign interference, which is referred to by defence and national security actors as the "grey zone" domain of national security operations, where traditional distinctions such as legal/illegal, ethical/unethical, and intrusive/non-intrusive may not apply clearly (Hribar et al., 2014).

In recent years, TikTok has exponentially risen in popularity, especially among young people. Between 2018 and 2022, the TikTok user base expanded by, on average, 340 million new active members each year (Buchholz, 2022). Its trajectory of growth reached a significant milestone when it surpassed one billion users in 2019, a feat attributed to the "digital boom" ignited by the Covid-19 pandemic (Jaipong, 2023). In 2021, TikTok surpassed Instagram's users, solidifying its position as a leading international social media platform (Buchholz, 2022).

This growth was narrated by two interconnected discourses that centred on risks to data security and political influence. For example, in their submission to the Australian Parliament, Lee and associates (2023) build a taxonomy of the severity and likelihood of these concerns, including Chinese censorship, data harvesting, narrative control (i.e. mis/dis information), privacy violations, political interference, surveillance, and intelligence operations.

TikTok's Cayman-headquartered corporate structure ties it to a China-based company Bytedance, that complies with Chinese censorship regulations (Jia & Ruan, 2020). Bytedance is strategically based in the Cayman Islands and owns both the China-based version of TikTok—Douyin (??)—as well as the international versions of the app. Due to this corporate structure, the Chinese government has the potential to access user data for Chinese state surveillance purposes (Bernot & Smith, 2023). However, TikTok (as the international facing version of the app, compared to the Chinese local version Douyin) is more compliant with the data protection guidelines driven by local legislation, as opposed to the domestic version of the app that tend to prioritise national security over individual rights to privacy (e.g. via increased in-app surveillance) (Jia & Ruan, 2020). In a March 2023 US congressional hearing, House Energy and Commerce Chair Cathy McMorris Rodgers opened the hearing by stating that "TikTok surveils us all and the Chinese Communist Party is able to use this as a tool to manipulate America as a whole" (The Department of Energy and Commerce, 2023). These concerns are central to the geopolitical and technological clash between the US, UK, Australia, the EU, and China, leading to concerns about national security, technological sovereignty, foreign interference, social media dominance, trade practices, and privacy.

2.2 Technological sovereignty and foreign interference

Technological sovereignty (sometimes referred to as digital, data, or cyber sovereignty, and often in interchangeable ways) has various and distinct meanings depending on the context in which it is used. We adopt the term technological sovereignty as it encompasses a broader range of technologies, with digital technologies being a subset of those. Couture and Toupin (2019, p. 295) define technological sovereignty as "some form of collective control on digital content and/or infrastructures". The concept of technological or digital sovereignty has been applied as a way towards individual and community ownership, control, and access to data (see for example, Mann et al., 2020a; and Pohle & Thiel, 2020). This notion is also linked to Indigenous and First Nations movements such as the Indigenous Data Sovereignty movement (Kukutai & Taylor, 2016).

The concept of technological sovereignty has been deployed by nation states and regions in the context of data localisation and security (see, for example, Bellanova et al., 2022). We focus on technological sovereignty as applied to *nation states* and consistent with historical conceptions of sovereignty as the authority within and over a specific territorial jurisdiction: "sovereignty is linked to the idea that states are autonomous and independent from each other: within their own boundaries, they are free to choose their own form of government and one state does not have the right to intervene in the internal affairs of another" (Krasner, 2001, p. 2).

Technological innovation, transnational/foreign surveillance, access to and control over data are forms of strategic and geopolitical advantage for nation states. The fear is that nation states and regions are losing control over technologies and data with consequences for their economies and national security. There have also been increasing attempts to assert and defend discrete forms of technological sovereignty, such as controls over 5G mobile communications as introduced above (da Ponte et al., 2023), cloud computing (Irion, 2013), and the transmission and (local versus cloud) storage of data. In addition, varied technological, political, diplomatic, legal, and regulatory approaches have been adopted to assert technological sovereignty, which range from technological (i.e. new undersea cables, encryption, and localised data storage) to non-technical (i.e. domestic industry support, international codes of conduct, and data protection laws) (Maurer et al., 2015, p. 1).

Arguments for technological sovereignty are motivated by several interconnected geopolitical, economic, national, and (cyber) security considerations. It has been argued in the EU that "a new approach to cybersecurity is emerging, in which the non-EU private sector can be perceived as much of a threat as foreign powers, and from whom digital sovereignty must be secured" (Farrand & Carrapico, 2022, p. 435). The Digital Single Market and recognition of the power of US technology companies and associated storage of data in the US (Fleming, 2021) contributes to these processes, in contrast with the visions of technological sovereignty in the US, Australia, and the UK that are directed at preventing or limiting foreign interference (Table 1).

Data localisation navigates a thin line between sovereignty and protectionism. The internet is said to be splintering and fragmenting due to a variety of reasons, including differing national interests and broader geopolitical dynamics. This phenomenon is referred to as the "splinternet" or "internet balkanisation." Data localisation can restrict international data flows by dictating "where and how [data] may be stored, processed or transferred" (Fraser, 2016, p. 359). While the splinternet threatens to reduce economic benefits of globalisation (Bauer et al., 2014), it is al-

so increasingly considered in the context of technological sovereignty and national economic benefit. For example, India's approach to a nationwide ban of TikTok reflects a determined approach to sovereignty via data localisation strategies (Kumar & Thussu, 2023). Whether or not data balkanisation would limit foreign surveillance activities is also not clear (Fraser, 2016, pp. 364–365).

Another important concept to consider, and which is related to geopolitical tensions, is the notion of foreign interference. Foreign interference has gained international importance in the wake of cyberattacks (Tuffley, 2023), harassment of overseas diasporas and political dissidents, dis/misinformation campaigns (Ryan et al., 2020), and attempts to influence political decision-making as well as elections (Lemke & Habegger, 2022). There is a continuum between foreign influence and *unlawful* foreign interference, in which states seek to gain influence in a transparent manner (such as diplomacy), compared to covert and coercive forms of interference (Mansted, 2021). Defining interference is difficult and policymakers face the challenge of striking a balance between a definition that is overly broad, potentially impeding freedom of expression and political engagement, and one that is too narrow to address emerging and evolving forms of behaviour that could hinder their broader international strategic interests (Berzina & Soula, 2020).

We define foreign interference as:

> activities conducted by or on behalf of a foreign power or state-level actor that are coercive, corrupting, deceptive, clandestine, or manipulative, with the intent to undermine the sovereignty (technological or otherwise), values, national interests, democratic institutions, and public confidence of a targeted country. Foreign interference poses a threat to technological sovereignty by manipulating or infiltrating a nation's technological infrastructure, compromising data integrity, and eroding control over information, thereby undermining the nation's ability to govern its digital space independently and posing risks to issues such as national security and privacy. Technological sovereignty involves a nation's control over its technologies and digital spaces to mitigate foreign interference and safeguard national interests.

Increased government and national security powers have been introduced to tackle foreign influence in political institutions (Chubb, 2023) and higher education (Cooney-O'Donoghue, 2023). Berzina and Soula (2020) discuss how the European Commission under President Ursula von der Leyen seeks to protect democratic systems and institutions from "external interference", including laws to combat disinformation (Berzina & Soula, 2020), and foreign interference in elections (Henschke

et al., 2020; Ringhand, 2021). Further research emphasises information warfare (Dowling, 2021, p. 384) and disinformation campaigns, which have often been driven by Russia (Lemke & Habegger, 2022). There is a lack of research on how responses to foreign interference specifically focus on the management of risks arising from social media platforms, and how they may compare internationally.

Critics argue that TikTok can collect and harvest vast amounts of data on citizens, which the Chinese government could covertly access, enabling espionage and the surveillance of government buildings, officials, or those with access to sensitive or classified information (Tuffley, 2023). For example, at present there is a US federal investigation into the tracking of Wall Street Journal's journalists that were reporting critically on TikTok (Gurman, 2023). Further, it has been argued that TikTok threatens democracy by promoting disinformation and pro-CCP narratives, while censoring information that challenges pro-CCP narratives (Ryan et al., 2020). Likewise, the FBI has expressed concern that TikTok could be used by the CCP to conduct data operations and traditional espionage, influence operations, and control devices via its software (Martina et al., 2023).

These interrelated concerns about technological sovereignty and foreign interference have prompted varying responses in the US, UK, Australia, and the EU, leading to the implementation of stricter regulations or outright bans, enhanced cybersecurity measures, and increased scrutiny of foreign investments and political activities to safeguard national sovereignty and democratic processes (Henschke et al., 2020; Ringhand, 2021; Table 1). These responses reflect a strong focus on activities carried out by foreign states that appear coercive, corrupting, deceptive, clandestine, and contrary to another nation's values, sovereignty, and the sanctity of its democratic institutions.

Table 1 below summarises the definitions and conceptualisation of technological sovereignty and foreign interference across the four jurisdictions analysed in this article.

Table 1: Definitions and conceptualisations of foreign interference and technological sovereignty in the AUKUS countries and the EU

	US	UK	AUSTRALIA	EU
FOREIGN INTERFERENCE	Includes covert actions by foreign governments to influence US political sentiment or public discourse. The aim is to spread	The National Security Bill 2023 defines foreign interference as malign activity carried out for, or on behalf of, or intended to benefit, a foreign power. It intends to sow discord, manipulate public discourse, discredit the political system,	The Australian Government explains that foreign interference occurs when activity carried out by, or on behalf of,	Activities are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the

	US	UK	AUSTRALIA	EU
	disinformation, sow discord, and ultimately, undermine confidence in democratic institutions and values (Federal Bureau of Investigations, n.d.).	promote bias in the development of policy, and undermine the safety or interests of the UK. A foreign state could seek to manipulate whether or how someone participates in an electoral event (Home Office, 2023).	a foreign power, is coercive, corrupting, deceptive or clandestine, and contrary to Australia's sovereignty, values, and national interests (Department of Home Affairs, 2023).	sovereignty, values, and interests of the EU (Directorate-General for Research and Innovation & European Commision, 2022).
TECHNOLOGICAL SOVEREIGNTY	While recognising its technical and data storage dominance, the United States is concerned about maintaining its technological sovereignty in the face of China's technological progress, which poses threats to national security and economic interests (Schüller & Schüler-Zhou 2020).	The UK Foreign Commonwealth and Development Office (2021) recognises the national security risks associated with foreign investment and the possibility of hostile foreign-owned entities undermining security interests or foreign ownership of strategically important assets and forms of domestic supply.	Australia does not have an explicit technological sovereignty strategy. However, Australia's Digital Government Strategy outlines "immediate data challenges" as risks to data sovereignty, data centre ownership, and the supply chain (Digital Transformation Agency, n.d.).	Technological sovereignty concerns the ability to exercise control over data and digital assets while being technologically independent of foreign suppliers. The EU works to create and manage digital infrastructures (sovereignty over the digital), as well as employing digital tools for the governance of European security (Bellanova et al., 2022).

3 Jurisdictional responses to restricting Chinese technologies and TikTok

3.1 United States

Since 2020, TikTok's presence in the US has been caught between discussions about geopolitical power, divestiture pressures, data security, foreign interference, and platform governance. The US approach to banning the sale of and forcing divestment from TikTok has been built on an *ad hoc* assortment of available laws and regulations that is tightly linked with preserving its political and economic interests of the US. The Committee on Foreign Investment (CFIUS) — an agency that reviews mergers, acquisitions, and other transactions that may have national security implications — was leveraged by the Trump administration in evaluating TikTok privacy risks after it acquired a US-based company Musical.ly in November 2017 (Feder, 2021). Previous CFIUS orders had set precedents in relation to data security and national security concerns: in 2019, Beijing Kunlun Tech Co. Ltd. was ordered to divest from the LGBTQI+ dating app Grindr due to access to sensitive personal information, and another Chinese company was ordered to divest owner-

ship interest from a company PatientsLikeMe that allowed people with similar medical conditions to locate each other (Feder, 2021). CFIUS provided a divestiture recommendation for TikTok to limit national security risks, which was the basis for the Trump administration to issue an executive order (List, 2022). This decision carried few details and has been widely critiqued as an overstretch of CFIUS' ever-expanding remit.

On 6 August 2020, Trump issued an executive order indicating how mobile applications developed and owned by Chinese companies continue "to threaten the national security, foreign policy, and economy of the United States"; Trump argued that all transactions of persons with TikTok need to be banned due to a "national emergency with respect to the information and communications technology and services supply chain" (Executive Office of the President, 2022). For Trump, TikTok was a technological representation of Chinese economic competition and dominance in the US, which became a strategy of his Presidency (Ashbee & Hurst, 2021). Trump's executive order was rejected as a threat to national security by US courts analysing both the Constitution and federal statutes to establish what does and does not constitute a national security emergency (Chander, 2023).

TikTok proceeded to partner with the computer technology company Oracle to locally hold US user data via an initiative called "Project Texas." This arrangement enabled US TikTok data to "communicate with the global TikTok service in controlled and monitored ways" (TikTok, n.d.). This form of data localisation can be viewed as part of a national technological and digital sovereignty strategy, whether articulated explicitly or more formally via regulatory actions (Kumar & Thussu, 2023). Additionally, TikTok opened "Transparency and Accountability Centers" digitally and in Los Angeles, considered an attempt to avoid a domestic ban (Grandinetti, 2021).

Prior to a 2023 Congressional hearing, the Biden administration continued with the hard stance of divestiture or TikTok running the risk of a nationwide ban in case of divestiture refusal. During the 2023 Congressional Hearing, TikTok's representative was presented with numerous questions about concerns over privacy, data harvesting, inappropriate content (for children), and the relationship of ByteDance and TikTok with the CCP. At the time of writing, a final decision on TikTok's operations in the US is pending.

Data transfer and misuse concerns have been observed by the US media which has fuelled political and regulatory action. One of the most important investigative stories was published by BuzzFeed reporters in June 2022 based on 80 internal

TikTok meetings (Baker-White, 2022a). The story built on 14 statements from nine TikTok employees and revealed that select staff at ByteDance in China were able to access US user data between September 2021 and January 2022. The story cites TikTok's Trust and Safety department's employee saying that "everything is seen in China" and a TikTok director referring to a "master admin" who "has access to everything." BuzzFeed's story triggered the March 2023 Congressional hearing (Energy and Commerce Committee & Chew, 2023).

In October 2022, Forbes reported that ByteDance's Internal Audit team planned to use location information to surveil individuals, in contravention of an executive order signed by Biden one month earlier that emphasised the risk of the potential for foreign-owned companies to undertake "surveillance, tracing, tracking, and targeting of individuals or groups of individuals, with potential adverse impacts on national security" (Baker-White, 2022b). In December 2022, Forbes disclosed that three journalists were targeted for surveillance who previously worked for BuzzFeed on critical technology stories. These reports were linked with TikTok's employee attempts to use location data to match the location of the journalists with potential sources that may be leaking TikTok's information. Surveillance of journalists has deleterious consequences to the operation of a free press, also weakening democracy (Harkin & Mann, 2023). TikTok's response centred on the function of internal audit to uncover potential misconduct (Baker-White, 2022b), but in December it admitted that journalist surveillance was "misconduct of certain individuals, who are no longer employed at ByteDance" (Baker-White, 2022c).

3.2 United Kingdom

TikTok is a matter of concern for UK policymakers. BuzzFeed's reporting resulted in a shift in articulating data transfer concerns. Previously TikTok was asked to confirm or deny data "transfer" issues that were usually met with statements such as the one offered by a TikTok executive Theo Bertram during UK parliamentary committee hearing in September 2020: "No employee in China can access TikTok data in the way that you are suggesting on behalf of the CCP to carry out mass surveillance" (Bertram, cited in Ryan, 2022). BuzzFeed's reporting revealed that, "the location in which any data is stored is immaterial if it can be readily accessed from China" (Ryan, 2022).

In early 2023, the Cabinet Office Ministers ordered a security review by a cabinet committee. Additionally, at the request of the security minister Tom Tugendhat, the National Cyber Security Centre (NCSC) of GCHQ, was involved with the review of TikTok's cybersecurity (Corfield, 2023). NCSC met TikTok representatives in Febru-

ary 2023 and concluded its investigation using a risk-based evaluation of TikTok's threat level (Corfield, 2023). In April 2023, the Director of the NCSC Richard Browne pinpointed the source of the concerns with data on publicly owned government devices, rather than individual risks, and signalled that this move is consistent with EU countries and the European Commission (Boland, 2023). NCSC's technical app evaluation did not reveal threats, but data access by TikTok employees in China implied a degree of risk of covert data access by China's intelligence agencies. This prompted the NCSC to recommend a risk-based approach (Boland, 2023).

In March 2023, TikTok was banned from all parliamentary devices through a joint decision by the commissions of both the House of Commons and Lords based on cybersecurity concerns around sensitive government information, but there was no commentary on the exact reasons (Hern, 2023). UK Prime Minister Rishi Sunak stated he will take "whatever steps are necessary" to protect Britain's security, as TikTok raises fear about national security concerns (Milmo & Crerar, 2023). Sunak also signalled strategic alignment with its allies: "We look at what our allies are doing" (Maclellan, 2023).

The UK's approach to TikTok has formed part of its broader response to foreign interference and national security, to mitigate the risks related to foreign state-sponsored disinformation campaigns through social media applications (see Home Office, 2023). The UK has been focused on cybersecurity and data governance, and its responses to TikTok's ties with the Chinese government have referenced the US approach.

3.3 Australia

Australia has responded to concerns about foreign interference, national security, and TikTok's relationship with the CCP by taking measures to protect government information and combat the spread of misinformation. The Australian response has also been largely aligned with and informed by the earlier responses to TikTok in the US and UK.

In April 2023, Australia's Attorney General, Mark Dreyfus, announced a ban on TikTok on government devices due to concerns that the CCP could gain access to the information of government employees. Dreyfus stated: "After receiving advice from intelligence and security agencies, today I authorised … a mandatory direction under the Protective Security Policy Framework to prohibit the TikTok app on devices issued by Commonwealth departments and agencies" (Dreyfus, 2023).

The Australian government is concerned about social media platforms promoting prejudice and hate, facilitating harassment, and dividing society. The Senate Select Committee on Foreign Interference through Social Media report in 2021 called for greater regulation of social media platforms to combat misinformation during democratic elections. Minister for Cyber Security Claire O'Neil has highlighted the challenges that arise from the use of technology companies based in countries with authoritarian regimes. In 2022, she noted: "It's not just about TikTok. […] The fact that we've got millions of Australians accessing an app where the usage of their data is questionable is very much a modern security challenge for the country, and no country in the world has found the easy solution for managing this" (Galloway, 2022). It should be noted that the Australian Competition and Consumer Commission (2019) has undertaken an inquiry into digital platforms more broadly, with a focus on media dominance in the creation of news and journalism, although highlighting many privacy concerns, and which has triggered a review into the federal *Privacy Act 1988* (Cth) that is ongoing.

Liberal National Party (Opposition) Senator James Paterson has been an advocate for greater restrictions on TikTok (Gailberger, 2022). Following the release of the BuzzFeed story in June 2022, Paterson submitted a formal letter to TikTok in July to inquire if Australian's data was also accessible in China. TikTok stated the Australian's data was stored in Singapore and the US, and access to that data is minimised and limited only to people who need the data "to do their jobs," confirming China-based access (Paterson, 2022). Paterson highlighted the risks of popular apps that collect sensitive information about users based in authoritarian countries requiring Australian government protection from potential data breaches and foreign interference (Paterson, 2023). In July 2023, Paterson led a series of Senate hearings on foreign interference via social media, during which the Senate also questioned representatives of TikTok Australia, revealing that the Australian TikTok managers had tried to obfuscate journalistic surveillance (Al-Nashar, 2023a) and that TikTok's China-based employees also had the ability to change the algorithm (Mason, 2023). The hearings also found that despite complaints having been lodged and foreign interference having been criminalised since 2018, the Australian Federal Police had only charged two people reporting difficulty of definitively establishing foreign actor involvement (Al-Nashar, 2023b).

At the time of writing, the Australian Office of Information is investigating TikTok's use of tracking pixels. The Attorney-General Mark Dreyfus has publicly stated that such activities are "particularly alarming given TikTok is beholden to the Chinese Communist Party and is required under China's intelligence laws to share informa-

tion" (as cited in the ABC, 2023). At present, and following the ACCC Digital Platforms Inquiry introduced above, the *Privacy Act 1988* (Cth) is currently undergoing reform.

3.4 European Union

The European Union (EU) General Data Protection Regulation (GDPR) is considered the global or gold standard for data protection regulation (although there are debates about this, see, for example, Mantelero, 2021). It also has introduced a range of measures to regulate Very Large Online Platforms and Search Engines via the Digital Services Act (DSA), and is leading the regulation of Artificial Intelligence with the introduction of the AI Act. Contrasting with the other national case studies above, the EU has primarily attempted to challenge the dominance of US platforms (for example, via the DSA), rather than specifically target or ban Chinese platforms, with the view to promote and protect *technological sovereignty*. At the EU level, only one top-down decision involved the ban of TikTok on government devices in February 2023, with some member states questioning the reasons behind the decision. The EU Commission's Corporate Management Board cited cybersecurity concerns and potential vulnerabilities (European Commission, 2023b) to justify this measure. Other EU responses to TikTok have been reliant on the rights-based laws that the European Commission uses to regulate all Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) (European Commission, 2023a).

A key distinction in platform regulation in the EU can be contrasted with the approach in the US, UK, and Australia. In 2022, the European Parliament and Council agreed to adopt the Digital Services Act (DSA) that came into effect in November 2022 and "regulates the obligations of digital services, including marketplaces, that act as intermediaries in their role of connecting consumers with goods, services, and content" (European Commission, 2024). This measure attempts to preserve and protect the Digital Single Market with individual member states' regulating online platforms, including non-EU actors operating within the European market (Cini & Czulno, 2022). US-based companies, including the "Big Five" (Google, Amazon, Meta, Microsoft, and Apple) were the focal point of these policy discussions because they store over 90% of "all the data in the Western world" (Fleming, 2021). On 13 April 2023, the Irish Data Protection Authority issued the largest GDPR fine of €1.2 billion to date to Meta for transfers on personal data to the US (European Data Protection Board, 2023).TikTok's governance has been an inevitable by-product of these new regulatory obligations and oversight structures that placed primary governance focus on US-based companies, potentially due to

US technological hegemony and associated geopolitical concerns (Gray, 2021).

The DSA mandates companies with more than 45 million users to comply with additional data security regulations and moves the regulatory mandate away from the supervision of individual member states to direct regulatory supervision by the European Commission (European Commission, 2023c). As a company with over 125 million users in the European Union, TikTok is under direct oversight by the European Commission. The EU has mediated complaints by member countries made against TikTok across several areas of concerns, ranging from consumer rights to cybersecurity.

Disinformation and misinformation also affected TikTok via a Code of Practice on Disinformation (herein, the Code). The Code uses the term "disinformation" to include information influence operations and interference by foreign actors (European Commission, 2022a). Hate speech removal on TikTok is monitored by the EU Commission's evaluation on the Code of Conduct on Countering Illegal Hate Speech Online, which TikTok joined as a signatory (Reynders, 2021). In 2022, TikTok was reportedly the only company to increase notice-and-action results from 82.5% in 2021 to 91.7% in 2022 (European Commission, 2022b).

Overall, the EU Commission uses a range of legal and regulatory measures—some mandated and some voluntary—to govern TikTok. During a public hearing in the European Parliament in May 2023, several members questioned the overnight decision that did not explicitly state cybersecurity concerns by noting that they did not want to "trust blindly" and felt "infantilised" (Goujard et al., 2023). Foreign interference is regulated via the Code of Practice on Disinformation that can launch investigations and result in fines.

4 Discussion and implications: politicisation or protection?

The AUKUS and EU examples show that TikTok raises similar national security, foreign interference, and privacy concerns in each jurisdiction we consider in this article. Since 2020, TikTok's representatives have evoked the language of "technological neutrality" and in doing so attempted to evade transparent communication about TikTok's data collection, access and use, a tactic that has historically been used by both Chinese and non-Chinese technology companies (Bernot, 2022). TikTok's reluctance to provide transparent answers about data governance has not been well received due to China's authoritarian nature, and the absence of trust, particularly among Australia, the UK, and the US, which stems from broader and

historical geopolitical tensions. In this context, the EU's conceptualisation of technological sovereignty threats and strategies to manage them is unique.

The specific responses to TikTok within each jurisdiction are shaped by the policy and regulatory tools available within each jurisdiction, and are also dependent on notions of foreign interference and technological sovereignty (as per Table 1). The US federal and state government actors have been aggressively pursuing various pathways to banning TikTok, efforts that culminated in the 2023 Congressional Hearing. Efforts to strengthen US privacy legislation voiced during the Hearing did not come to fruition, and TikTok representatives are now scheduled to appear in the US Senate on child sex exploitation in early 2024, along with Meta, Snap, and Discord (Shepardson, 2023).

The responses to TikTok in the US are similar to those in the UK and Australia which is perhaps unsurprising given that they operate in numerous strategic intelligence and military alliances (i.e. ANZUS, AUKUS and the Five Eyes). As our analysis has demonstrated, the responses of the AUKUS countries to TikTok were politicised as evidenced by scare campaigns, moral panics, xenophobic overtones, and knee-jerk political reactions described in the national examples presented above. This can be compared with the EU approach, which has tended to be rights-driven with a focus on challenging US dominance and regulating all VLOPs, rather than specific concerns about China, and reflects a more protectionist approach to internet governance, underpinned by the right to data protection (*Charter of Fundamental Rights*, 2012, Article 8) and protecting the digital single market.The responses to TikTok in each jurisdiction are also shaped by the conception of technological sovereignty. In the US, this loosely encompasses issues of economic and national security (Gray, 2021; Slawotsky, 2021; Table 1), broadly positioning China's technical progress as a threat to its own technological hegemony (Schüller & Schüler-Zhou, 2020).

Concerns over foreign interference have been highly salient in Australia, driven by China's threat to domestic security, and as we have demonstrated in this article, TikTok now forms an important element. In this way, Australia may be influenced by the US' securitised framing and approach, with China presented as a threat to domestic security. This means that technological sovereignty as conceived in this context primarily seeks to mitigate security threats, rather than prioritising rights to data protection and privacy more broadly (Mann et al., 2018). It is worth noting that rights-based approaches are absent, underdeveloped, or unenforceable in some of the AUKUS countries' legal frameworks (especially Australia which lacks comprehensive human rights protections at the federal level) (see for example,

Mann et al., 2020b). However, as mentioned above, there are currently investigations into TikTok and wider reform processes of the *Privacy Act 1988* (Cth) currently underway, although at this stage it is not clear what the outcome of this investigation will be, nor how effective reforms to the *Privacy Act 1988* (Cth) will be in regulating TikTok. It is important to consider that the US largely has a near-monopoly on the Western world's data (Fleming, 2021) and Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) (European Commission, 2023a). This may help understand why the focus on national security and economic interests present in the US, UK and Australia's conceptualisation of technological sovereignty was not as strongly emphasised in the EU.

These findings also connect to research that has identified that the US prioritises the socio-economic benefits of data economies over privacy risks and consequently adopts a market-based approach to governance (Guay & Birch, 2022). This differs from the EU, that tends to focus on privacy rights and data protection using an ex-ante and state-market model and also focuses on protecting the EU digital market, primarily from US hegemony and technological dominance. The EU has presented one possible alternative in positioning itself as a state that seeks to *protect* citizens and its wider digital markets, rather than *attack* specific platforms connected to geopolitically non-allied governments. This highlights the importance of considering geopolitical dimensions when analysing regulatory responses to social media platforms. Indeed, the EU conceptualisation of technological sovereignty differs in that it is more concerned with the dominance of US technology companies and the protection of EU citizens' data. Bellanova et al. (2022, p. 337) explain that digital sovereignty has both direct and indirect implications for European security: "the EU attempts to develop and control digital infrastructures (sovereignty *over* the digital), as well as the use of digital tools for European security governance (sovereignty *through* the digital)". The President of the EU has identified digital policy as one of the key political priorities of her 2019–2024 term in office and pledged that the EU will achieve "technological sovereignty" in critical areas (Madiega, 2020). This is consistent with the broader EU approach to technological sovereignty that concerns the region's ability to exercise control over data and digital assets while being technologically independent of foreign suppliers, as shown in Table 1 (see also, Bellanova et al., 2022). This is also evident through the EU's moves to construct new supervisory infrastructure for 19 Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), all of which are non-EU owned (European Commission, 2023a). Such policies will undoubtedly have important implications for internet governance and policy internationally and the concepts of technological sovereignty and foreign interference in wider geopo-

litical contexts can assist with understanding and critiquing such developments.

In this article, we have shown how the concepts of technological sovereignty and foreign interference interact with Chinese technologies and platforms, as well as the regulatory responses introduced by a small sample of Western nation states to assert and protect their technological sovereignty. We argue that it is important to consider wider geopolitical tensions and strategic interests as these shape the responses that states (or regions) seek to adopt. Through this analysis we have shown that the US is more prone to *attack* particular platforms connected to geopolitically non-allied governments (such as China) both because of national security concerns and threatened national economic interests; the EU, on the other hand, aims to position itself as a state that seeks to *protect* citizens and the wider digital market through a regime that attempts to create technological independence, and largely from the US. These findings connect to recent research on the divergent socio-technical imaginaries of personal data in the US and the EU, which identified that the US prioritises the socio-economic benefits of data economies over privacy risks and adopting a post hoc and market-based approach (Guay & Birch, 2022). This differs from the EU that focuses on privacy rights and data protection using an ex-ante and state-market model (Guay & Birch, 2022). The UK and Australia fall somewhere in the middle, speaking to both the need to strengthen their regulatory regimes as well as address national security threats, following the US lead. These socio-technical imaginaries and conceptions of personal data and the value that is ascribed to it are also relevant to consider because they have implications for regulation and policy as introduced to respond to risks and threats to technological sovereignty. We acknowledge that our focus is limited to Western jurisdictions and geopolitical dimensions between Western allies and China and further research into such dynamics is important to understand variations in approaches to internet governance.

5 Conclusion

In this article we have shown that AUKUS countries presented a political narrative focused on the threats presented by China and TikTok's links with the CCP. This, however, might be occurring at the risk of overshadowing other foreign interference risks, including the risks posed by Western social media companies. We also emphasise that framing foreign interference threats as solely originating in China creates a policy blind spot, including that of mis-/disinformation and election interference, for example, the Facebook/Cambridge Analytica case illustrated how a US-based company can engage in harvesting user profiles for election manipula-

tion (Manokha, 2018). This is not to say that CCP's capability to have foreign interference influence should be taken lightly. For example, the CCP has been found to engage in information operations on social media (Ryan et al., 2020). The various responses to TikTok analysed in this article suggest that approaches to internet governance should adopt a more holistic and rights-based approach to regulation and policy. A "whack-a-mole" approach (Bennett Moses, 2023) to banning or blocking individual platforms and directed at specific countries or platforms considered to present a threat to technological sovereignty will not suffice as a long-term solution that *protects* citizens and their personal data as such approaches are founded in wider geopolitical attempts to assert and maintain international power and dominance over the internet. Although the EU has its own investments by combatting US technology dominance with regulatory power as evidenced by the EU single digital market, the EU approach presents a less politicised alternative by adopting a rights-based protective framework through, for example, the DSA and GDPR. Finally, these findings present an opportunity to critically reflect on notions of technological sovereignty which focus on the wins and losses of nation states and frame data as a resource for exploitation for national benefit, geopolitical advantage, and corporate extraction. They also show how the concepts of technological sovereignty and foreign interference can be helpful in understanding and problematising regulatory responses.

ACKNOWLEDGEMENTS

The authors express their gratitude to Dr. Ian Warren for his invaluable contributions in editing and providing insightful feedback on an earlier version of this work. Additionally, we extend our thanks to the reviewers and the Managing Editor Frédéric Dubois for their constructive feedback, which significantly enhanced the overall quality of the manuscript.

References

ABC. (2023, December 28). Claims TikTok siphons personal data of non-users without consent examined by Australian Information Commissioner. *ABC News*. https://www.abc.net.au/news/2023-12-28/tiktok-personal-information-data-scraping-australian-authorities/103271042

Al-Nashar, N. (July 11, 2023a). TikTok executives frustrate parliamentary inquiry with 'reluctance to acknowledge basic facts'. *ABC News*. https://www.abc.net.au/news/2023-07-11/tiktok-says-it-doesnt-know-if-its-headquarters-are-in-china/102589206

Al-Nashar, N. (July 13, 2023b). AFP says laws make it difficult to lay charges for foreign interference

over social media. *ABC News*. https://www.abc.net.au/news/2023-07-13/no-charges-for-foreign-interference-through-social-media/102594722

Ashbee, E., & Hurst, S. (2021). The Trump administration and China: Policy continuity or transformation? *Policy Studies*, *42*(5–6), 720–737. https://doi.org/10.1080/01442872.2021.1919299

Australian Competition and Consumer Commission. (2019). *Digital platforms inquiry—Final report* [Report]. Government of Australia. https://www.accc.gov.au/about-us/publications/digital-platforms-inquiry-final-report

Bagshaw, E. (2023, February 10). Beijing says Australia's removal of cameras an 'abuse of state power'. *The Sydney Morning Herald*. https://www.smh.com.au/world/asia/beijing-says-australia-s-removal-of-cameras-an-abuse-of-state-power-20230210-p5cjjq.html

Baker-White, E. (June 17, 2022a). Leaked audio from 80 internal TikTok meetings shows that US user data has been repeatedly accessed from China. *Buzzfeed News*. https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access

Baker-White, E. (October 20, 2022b). Tiktok parent Bytedance planned to use Tiktok to monitor the physical location of specific American citizens. *Forbes*. https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=5db502696c2d

Baker-White, E. (December 22, 2022c). TikTok spied on Forbes journalist. *Forbes4*. https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=d1db48f7da57

Bauer, M., Lee-Makiyama, H., Marel, E., & Verschelde, B. (2014). *The costs of data localisation: Friendly fire on economic recovery* (Research Report No. 3/2014; ECIPE Occasional Paper). European Centre for International Political Economy (ECIPE). https://www.econstor.eu/handle/10419/174726

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*, *31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887

Belot, H. (2023, February 9). Chinese-made security cameras to be removed from Australian government buildings. *The Guardian*. https://www.theguardian.com/australia-news/2023/feb/09/chinese-made-security-cameras-to-be-removed-from-australia-government-buildings

Bennet Moses, L. (2023, April 13). Australia needs a robust cybersecurity overhaul – not whack-a-mole bans on apps like TikTok. *The Conversation*. https://theconversation.com/australia-needs-a-robust-cybersecurity-overhaul-not-whack-a-mole-bans-on-apps-like-tiktok-203158

Bernot, A. (2022). Transnational state-corporate symbiosis of public security: China's exports of surveillance technologies. *International Journal for Crime, Justice and Social Democracy*, *11*(2), 159–173. https://doi.org/10.5204/ijcjsd.1908

Bernot, A., & Smith, M. (2023). Understanding the risks of China-made CCTV surveillance cameras in Australia. *Australian Journal of International Affairs*, *77*(4), 380–398. https://doi.org/10.1080/10357718.2023.2248915

Bernot, A., & Walsh, P. (2023, May 18). Is China out to spy on us through drones and other tech? Perhaps that's not the question we should be asking. *The Conversation*. https://theconversation.com/is-china-out-to-spy-on-us-through-drones-and-other-tech-perhaps-thats-not-the-question-we-should-be-asking-205576

Berzina, K., & Soula, E. (2020). *Conceptualizing foreign interference in Europe* [Report]. German

Marshall Fund: Alliance for Securing Democracy. https://securingdemocracy.gmfus.org/what-is-foreign-interference-conceptualizing-foreign-interference-in-europe/

Boland, L. (2023, April 21). National Cyber Security Centre tells Government departments to avoid TikTok on official devices. *The Journal*. https://www.thejournal.ie/tiktok-official-devices-cyber-security-6049733-Apr2023/

Buchholz K. (2022). *The rapid rise of TikTok* [Infographic]. Statista. https://www.statista.com/chart/28412/social-media-users-by-network-amo/

Chander, A. (2023). Trump v. Tiktok. *Vanderbilt Journal of Transnational Law*, *55*(5), 1145–1176.

Charter of Fundamental Rights of the European Union. (2012). *Official Journal*, C326, 26 October, 391–407. http://data.europa.eu/eli/treaty/char_2012/oj

Chubb, A. (2023). The securitization of 'Chinese influence' in Australia. *Journal of Contemporary China*, *32*(139), 17–34. https://doi.org/10.1080/10670564.2022.2052437

Cini, M., & Czulno, P. (2022). Digital single market and the EU competition regime: An explanation of policy change. *Journal of European Integration*, *44*(1), 41–57. https://doi.org/10.1080/07036337.2021.2011260

Clayton, J. (2023, March 24). TikTok CEO Shou Zi Chew's Congress showdown: Five takeaways. *BBC News*. https://www.bbc.com/news/65047087

Cooney-O'Donoghue, D. (2024). The politics of STEMM collaboration between Australia and China: National security, geopolitics, and academic freedom. *Asian Studies Review*. https://doi.org/10.1080/10357823.2023.2294800

Corfield, G. (2023, March 14). Minister orders GCHQ review of TikTok over national security fears. *The Telegraph*. https://www.telegraph.co.uk/business/2023/03/14/minister-orders-gchq-review-tiktok-national-security-fears/

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

da Ponte, A., Leon, G., & Alvarez, I. (2023). Technological sovereignty of the EU in advanced 5G mobile communications: An empirical approach. *Telecommunications Policy*, *47*(1), Article 102459. https://doi.org/10.1016/j.telpol.2022.102459

Department Home Affairs. (2023). *Australia's counter foreign interference strategy* [Strategy]. Australian Government. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-strategy

Digital Transformation Agency. (n.d.). *Whole-of-government hosting strategy* [Strategy]. Australian Government. https://www.dta.gov.au/our-projects/hosting-strategy/overview

Dowling, M.-E. (2021). Democracy under siege: Foreign interference in a digital era. *Australian Journal of International Affairs*, *75*(4), 383–387. https://doi.org/10.1080/10357718.2021.1909534

Dreyfus, M. (2023). *TikTok ban on Government devices* [Media release]. Australian Government. https://ministers.ag.gov.au/media-centre/tiktok-ban-government-devices-04-04-2023

European Commission. (November 24, 2022a). *Q&A: Guidance to strengthen the Code of Practice on Disinformation* [Guidance]. European Commission. https://digital-strategy.ec.europa.eu/en/policies/qa-code-practice-disinformation

European Commission. (November 24, 2022b). *EU Code of Conduct against online hate speech: Latest evaluation shows slowdown in progress* [Press release]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7109

European Commission. (April 25, 2023a). *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines* [Press release]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413

European Commission. (February 23, 2023b). *Commission strengthens cybersecurity and suspends the use of TikTok on its corporate devices* [Press release]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1161

European Commission. (June 6, 2023c). *The Digital Services Act package* [Policy brief]. European Commission. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

European Commission. (2024). *Questions and answers on the Digital Services Act** [Explainer]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

European Commission & Directorate-General for Research and Innovation. (2022). *Tackling R&I foreign interference* [Staff working document]. Publications Office of the European Union. https://data.europa.eu/doi/10.2777/513746

European Data Protection Board. (2023). *1.2 billion euro fine for Facebook as a result of EDPB binding decision* [Press release]. European Union. https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Executive Office of the President. (2020). *Addressing the threat posed by TikTok, and taking additional steps to address the national emergency with respect to the information and communications technology and services supply chain* (Executive Order 13942; Presidential Document, pp. 48637–48639). Federal Register. https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Feder, A. (2021). A cull in a china shop: How CFIUS made TikTok a national security problem. *Cardozo International and Comparative Law Review*, *5*, 627–670. https://heinonline.org/HOL/P?h=hein.journals/icpelr5&i=645

Federal Bureau of Investigations. (n.d.). *Combating foreign influence*. https://www.fbi.gov/investigate/counterintelligence/foreign-influence

Fleming, S. (2021, March 15). What is digital sovereignty and why is Europe so interested in it? *World Economic Forum: Agenda.* https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/

Fraser, E. (2016). Data localisation and the balkanisation of the internet. *SCRIPTed*, *13*(3), 359–373. https://doi.org/10.2966/scrip.130316.359

Full Committee Hearing: "TikTok: How Congress can safeguard American data privacy and protect children from online harms (2023). https://energycommerce.house.gov/events/full-committee-hearing-tik-tok-how-congress-can-safeguard-american-data-privacy-and-protect-children-from-online-harms

Gaida, J., Wong Leung, J., Robin, S., & Cave, D. (2023). *ASPI's critical technology tracker* [Report]. Australian Strategic Policy Institute. https://www.aspi.org.au/report/critical-technology-tracker

Gailberger, J. (2022, October 11). TikTok fear reaches new heights in suburbs. *The Herald Sun*. https://www.heraldsun.com.au/news/victoria/tiktok-fear-reaches-new-heights-in-suburbs/news-story/669c56fe6c6e935769555439eba47045

Galloway, A. (2022, September 4). Home Affairs to review data harvesting by TikTok and WeChat. *The Sydney Morning Herald*. https://www.smh.com.au/politics/federal/home-affairs-to-review-data-harvesting-by-tiktok-and-wechat-20220902-p5bf18.html

Goujard, C., Wax, E., & Haeck, P. (2023, March 3). Brussels banned TikTok. *Politico*. https://www.politico.eu/article/eu-brussels-ban-tiktok-europe-has-questions/

Grandinetti, J. (2023). Examining embedded apparatuses of AI in Facebook and TikTok. *AI & Society*, *38*, 1273–1286. https://doi.org/10.1007/s00146-021-01270-5

Gray, J. E. (2021). The geopolitics of 'platforms': The TikTok challenge. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1557

Guay, R., & Birch, K. (2022). A comparative analysis of data governance: Socio-technical imaginaries of digital personal data in the USA and EU (2008–2016). *Big Data & Society*, *9*(2). https://doi.org/10.1177/20539517221112925

Gurman, S. (2023, March 17). Justice department probes TikTok's tracking of U.S. journalists. *The Wall Street Journal*. https://www.wsj.com/articles/justice-department-probes-tiktoks-tracking-of-u-s-journalists-d7e47665

Harkin, D., & Mann, M. (2023). Electronic surveillance and australian journalism: Surveillance normalization and emergent norms of information security. *Digital Journalism*. https://doi.org/10.1080/21670811.2023.2220366

Henschke, A., Sussex, M., & O'Connor, C. (2020). Countering foreign interference: Election integrity lessons for liberal democracies. *Journal of Cyber Policy*, *5*(2), 180–198. https://doi.org/10.1080/23738871.2020.1797136

Hern, A. (2023, March 23). TikTok to be banned from UK parliamentary devices. *The Guardian*. https://www.theguardian.com/technology/2023/mar/23/tiktok-to-be-banned-from-uk-parliamentary-devices

Home Office. (2023). *Foreign interference: National Security Bill factsheet* [Policy paper]. Government of the United Kingdom. https://web.archive.org/web/20230515124442/http://www.gov.uk/government/publications/national-security-bill-factsheets/foreign-interference-national-security-bill-factsheet

Hribar, G., Podbregar, I., & Ivanuša, T. (2014). OSINT: A "grey zone"? *International Journal of Intelligence and CounterIntelligence*, *27*(3), 529–549. https://doi.org/10.1080/08850607.2014.900295

Ingram, D. (2022, December 30). Biden signs TikTok ban for government devices, setting up a chaotic 2023 for the app. *NBC News*. https://www.nbcnews.com/tech/tech-news/tiktok-ban-biden-government-college-state-federal-security-privacy-rcna63724

Irion, K. (2013). Government cloud computing and national data sovereignty. *Policy & Internet*, *4*(3–4), 40–71. https://doi.org/10.1002/poi3.10

Jaipong, P. (2023). Business model and strategy: A case study analysis of TikTok. *Advance Knowledge for Executives*, *2*(1), 1–18.

Jia, L., & Ruan, L. (2020). Going global: Comparing Chinese mobile applications' data and user privacy governance at home and abroad. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1502

Krasner, S. D. (Ed.). (2001). *Problematic sovereignty: Contested rules and political possibilities*. Columbia University Press. https://doi.org/10.7312/kras12178

Kukutai, T., & Taylor, J. (Eds.). (2016). *Indigenous Data Sovereignty: Toward an agenda*. ANU Press. https://doi.org/10.22459/CAEPR38.11.2016

Kumar, A., & Thussu, D. (2023). Media, digital sovereignty and geopolitics: The case of the TikTok ban in India. *Media, Culture & Society*, *45*(8), 1583–1599. https://doi.org/10.1177/01634437231174351

Lee, R., Luttrell, P., Johnson, M., & Garnaut, J. (2023). *TikTok, ByteDance, and their ties to the Chinese Communist Party: Submission to the Senate Select Committee on Foreign Interference through Social Media* (Report Submission 34). Select Committee on Foreign Interference through Social Media. https://t.co/ROPtMMud89

Lemke, T., & Habegger, M. W. (2022). Foreign interference and social media networks: A relational approach to studying contemporary russian disinformation. *Journal of Global Security Studies*, *7*(2), Article ogac004. https://doi.org/10.1093/jogss/ogac004

List, S. (2022). Is national security a threat to TikTok? *Seton Hall Legislative Journal*, *46*(173), 173–220. https://heinonline.org/HOL/P?h=hein.journals/sethlegj46&i=173

Maclellan, K. (2023, March 14). UK's National Cyber Security Centre reviewing TikTok risks, minister says. *Reuters*. https://www.reuters.com/world/uk/uks-national-cyber-security-centre-reviewing-tiktok-risks-minister-says-2023-03-14/

Madiega, T. (2020). *Digital sovereignty for Europe* (Briefing PE 651.992; EPRS Ideas Paper, pp. 1–12). European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Mann, M., Daly, A., Wilson, M., & Suzor, N. (2018). The limits of (digital) constitutionalism: Exploring the privacy-security (im)balance in Australia. *International Communication Gazette*, *80*(4), 369–384. https://doi.org/10.1177/1748048518757141

Mann, M., Mitchell, P., Foth, M., & Anastasiu, I. (2020a). #BlockSidewalk to Barcelona: Technological sovereignty and the social license to operate smart cities. *Journal of the Association for Information Science and Technology*, *71*(9), 1103–1115. https://doi.org/10.1002/asi.24387

Mann, M., Daly, A., & Molnar, A. (2020b). Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1499

Manokha, I. (2018). Surveillance: The DNA of platform capital—The case of Cambridge Analytica put into perspective. *Theory & Event*, *21*(4), 891–913. https://doi.org/10.1353/tae.2018.0054

Mansted, K. (2021). *The domestic security grey zone: Navigating the space between foreign influence and foreign interference* (National Security College Occasional Paper) [Report]. Australian National University. https://nsc.crawford.anu.edu.au/publication/18456/domestic-security-grey-zone-navigating-space-between-foreign-influence-and-foreign

Mantelero, A. (2021). The future of data protection: Gold standard vs. Global standard. *Computer Law & Security Review*, *40*, 1–5. https://doi.org/10.1016/j.clsr.2020.105500

Martina, M., Zengerle, P., & Dunham, W. (2023, March 9). FBI chief says TikTok 'screams' of US national security concerns. *Reuters*. https://www.reuters.com/technology/fbi-chief-says-tiktok-screams-us-national-security-concerns-2023-03-08/

Mason, M. (2023, June 5). TikTok code being worked on from China prompts fresh alarm. *Australian Financial Review*. https://www.afr.com/technology/tiktok-code-being-worked-on-from-china-prompts-fresh-alarm-20230328-p5cvu1

Maurer, T., Skierka, I., Morgus, R., & Hohmann, M. (2015). Technological sovereignty: Missing the point? *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 53–68. https://doi.org/10.1109/CYCON.2015.7158468

McCallum, S. (2023, February 23). European Commission bans TikTok on staff devices. *BBC News*. https://www.bbc.com/news/technology-64743991

Milmo, D., & Crerar, P. (2023, March 13). Rishi Sunak hints at TikTok ban from UK government devices. *The Guardian*. https://www.theguardian.com/technology/2023/mar/13/tiktok-would-be-disappointed-if-uk-banned-app-on-official-devices

Neilson, M. (2023, March 17). TikTok app banned on phones of New Zealand MPs by Parliamentary Service amid security concerns. *The New Zealand Herald*. https://www.nzherald.co.nz/nz/politics/tiktok-app-banned-on-phones-of-new-zealand-mps-by-parliamentary-service-amid-security-concerns/JVIKGCDSNBHSXKV6ATPKVFSO4E/

Paterson J. (2023). Haphazard TikTok bans. *Sky News*. https://james-paterson.webflow.io/news/haphazard-tiktok-bans-tanscript-credlin

Paterson, J. [@SenPaterson]. (2022, July 13). *I've written to @tiktokaustralia following revelations in the US that user data is accessible in mainland China, putting it within.*. [Image attached] [Tweet]. X. https://archive.md/g70jF

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Reynders, D. (2021). *Countering illegal hate speech online: 6th evaluation of the Code of Conduct* [Factsheet]. Directorate-General for Justice and Consumers, European Commission. https://commission.europa.eu/system/files/2021-10/factsheet-6th-monitoring-round-of-the-code-of-conduct_october2021_en_1.pdf

Ringhand, L. A. (2021). Foreign election interference: Comparative approaches to a global challenge. *Election Law Journal: Rules, Politics, and Policy*, *20*(1), 1–9. https://doi.org/10.1089/elj.2020.0683

Roberts, A., & Lamp, N. (2021). *Six faces of globalization: Who wins, who loses and why it matters*. Harvard University Press. https://doi.org/10.2307/j.ctv33mgbxx

Ryan, F. (2022, July 14). It's time TikTok Australia came clean. *The Strategist*. https://www.aspistrategist.org.au/its-time-tiktok-australia-came-clean/

Ryan, F., Fritz, A., & Impiombato, D. (2020). *TikTok and WeChat: Curating and controlling global information flows* (Policy Brief Report No. 37/2020). Australian Strategic Policy Institute. https://ccn.unistra.fr/websites/ccn/documentation/Cybersecurite/PB37-TikTok_and_WeChat_-_Curating_and_controlling_global_information_flows.pdf

Sabbagh, D. (2023, March 16). UK bans TikTok from government mobile phones. *The Guardian*. https://www.theguardian.com/technology/2023/mar/16/uk-bans-tiktok-from-government-mobile-phones

Schüller, M., & Schüler-Zhou, Y. (2020). *United States-China decoupling: Time for European tech sovereignty* (Research Report Number 7; GIGA Focus Asia). German Institute for Global and Area Studies (GIGA). https://www.jstor.org/stable/resrep28518

Shepardson, D. (2023, November 29). TikTok, Meta, X CEOs to testify at US Senate hearing in January. *Reuters*. https://www.reuters.com/technology/social-media-ceos-testify-us-senate-hearing-january-2023-11-29/

Slawotsky, J. (2021). The fusion of ideology, technology and economic power: Implications of the emerging new United States National Security conceptualization. *Chinese Journal of International Law*, *20*(1), 3–62. https://doi.org/10.1093/chinesejil/jmab007

The Department of Energy and Commerce. (2023). *Chair Rodgers to TikTok CEO: "Your platform should be banned"* [Hearing excerpt]. https://energycommerce.house.gov/posts/chair-rodgers-to-tik-tok-ceo-your-platform-should-be-banned

TikTok. (n.d.). *About Project Texas*. TikTok US Data Security. https://archive.md/80gsD

Treasury Board of Canada Secretariat. (2023). *Statement by Minister Fortier announcing a ban on the use of TikTok on government mobile devices* [Statement]. https://www.canada.ca/en/treasury-board-secretariat/news/2023/02/statement-by-minister-fortier-announcing-a-ban-on-the-use-of-tiktok-on-government-mobile-devices.html

Tuffley, D. (2023, April 4). Why was TikTok banned on government devices? An expert on why the security concerns make sense. *The Conversation*. https://theconversation.com/why-was-tiktok-banned-on-government-devices-an-expert-on-why-the-security-concerns-make-sense-202339

UK Foreign Commonwealth and Development Office. (2021). *FCDO's role in understanding national security risk* [Report]. UK Parliament. https://publications.parliament.uk/pa/cm5802/cmselect/cmfaff/197/19705.htm

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

cnrs centre internet et societe

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya

University of Tartu Johan Skytte Institute of Political Studies