Indian Journal of Law and Technology

Volume 17 | Issue 1 Article 1

2021

Building Digital Walls and Making Speech and Internet Freedom (or Chinese Technology) Pay for It

Building Digital Walls and Making Speech and Internet Freedom (or Chinese Technology) Pay for It

An Assessment of the US Government's Attempts to Ban TikTok, WeChat, and Other Chinese Technology

Apratim Vidyarthi & Rachel Hulvey***

Abstract *The Trump Administration's bans on Tik Tok and WeChat were the culmination in a line of escalating moves between the US and China that resulted in the US raising digital walls at home, in contrast to long-standing American foreign policy favouring Internet Freedom. This article examines the rationale cited by the US government for these digital walls, including threats of Chinese government access to American consumer data, the possibility of Chinese censorship on apps used by Americans, Chinese access to American government employees' data and military networks, and the ability of the Chinese government to interfere with American elections and spread disinformation. Our analysis suggests that of these threats, only the threat of access to government employees' data and military networks is sufficiently narrow and acutely rooted in reality so much so that the threat could possibly legally justify banning a foreign technology. However, even that analysis is close and rife with uncertainties.*

More broadly, the tools at the US government's disposal—IEEPA, Congressional lawmaking authority, and CFIUS review—encourage the use of such flimsy rationale and a lack of transparency, which ultimately promotes such broad bans; and the costs of these bans are dear. There may be First Amendment implications, and at the very least, a chilling of speech. There are also significant impacts on American foreign policy, from legitimizing the Chinese strategy of cybersovereignty and government regulation, to the creation of incentives to

* Apratim Vidyarthi: J.D. Candidate, 2022, University of Pennsylvania Law School.
** Rachel Hulvey: Ph.D. Candidate, Political Science, University of Pennsylvania.

Special thanks to Sarah Pierce, who provided guidance, review, and direction in our analysis and made this piece possible. Our gratitude also goes to the editors of the Indian Journal of Law and Technology for their hard work, edits, and advice.

localize data in a manner that might undermine American law enforcement efforts.

Introduction

The Internet is not a series of tubes.[1] Instead, it is a source of information and international communications, a new frontier of warfare, and the eternal source of memes[2]—all untethered to any geographical or earthly border. This analogy of a borderless internet is closely linked with the concept of free speech. In 2010, then-Secretary of State Hillary Clinton outlined the US commitment to internet freedom, including fundamental rights to access information under Article 19 of the Universal Declaration of Human Rights.[3] Expressing optimism towards the potential of technology, Clinton described the internet as a tool that enables democratic expression, echoing US Supreme Court rulings that describe the internet as the "modern public square."[4]

Despite early optimism that the internet is a space that amplifies rights to free expression, Clinton argued that governments present new threats to fundamental rights enshrined in international law, through measures that manipulate the flow of information across borders. Speaking in the language of the Cold War, Clinton described "virtual walls" that are "cropping up in

---

1 'The Daily Show with Jon Stewart: From Here to Neutrality' (*Comedy Central*, 26 October 2009) <https://www.cc.com/video/blvwyz/the-daily-show-with-jon-stewart-from-here-to-neutrality> accessed 24 April 2021.

2 See eg 'Rickroll' (*Know Your Meme*, 2008) <https://knowyourmeme.com/memes/rickroll> accessed 24 April 2021.

3 Daniel Joyce, 'Internet Freedom and Human Rights' (2015) 26 Eur J Intl L 493.

4 *Packingham v North Carolina* 2017 SCC OnLine US SC 72 : 198 L Ed 2d 273 : 137 S Ct 1730, 1737 : 582 US (2017).

the place of visible walls."[5] Government policies that either prevented access to particular websites or otherwise limited the flow of information constituted "a new information curtain . . . descending across much of the world."[6]

Although the US has long worked to prevent the rise of such digital walls abroad, on August 6, 2020, President Trump signed Executive Orders 13942[7] and 13943,[8] banning the popular video social media app TikTok and the Chinese messaging app WeChat respectively, citing national security risks. These bans were the next step in escalating tensions between the US and China. But the bans were also precarious—becoming tied up in courts, where the companies were ultimately granted temporary injunctions while litigation on the merits took place.[9] As of the time of writing, the Trump Administration—like a short TikTok video—has come to an end, and the bans have been revoked.[10]

However, the strategy of such bans is not short-lived, and instead poses serious risks to speech and the structure of the internet. Digital technology is now the primary avenue of expression, and government interference into which digital avenues are available for self-expression raises censorship and freedom of expression concerns regarding the government's interference with speech. While our mental perception of censorship is that a government writes what people within its borders see—whether in Orwell's 1984, The Interview's caricature of Kim Jong Un's cultural censorship, or the "lightly redacted" page 20 of the Mueller Report[11]—the concept of government regulation of speech is no longer so straightforward. Instead, it can be something as subtle as banning apps that are the primary means of communication for millions, under the pretext of security risks, while actually intended as a foreign power tool against foreign adversaries.

These threats to ban technology also hold long-term foreign policy implications. The US Internet Freedom foreign policy was initially designed to

---

5 Hillary Rodham Clinton, US Secretary of State, 'Remarks on Internet Freedom, Address Before the Newseum' (*US State Department*, 21 January 2010) <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm> accessed 18 April 2021.

6 ibid.

7 Exec Order No 13942, 85 Fed Reg 48637 (Aug 6 2020).

8 Exec Order No 13943, 85 Fed Reg 48637 (Aug 6 2020).

9 *Tiktok Inc v Trump* 490 F Supp 3d 73, 2020 US Dist. LEXIS 177250 at *26 (DDC 2020) [hereinafter *TikTok v Trump*] (providing an injunction for TikTok); *US WeChat Users All v Trump* 488 F Supp 3d 912 : 2020 US Dist. LEXIS 172816 at *34 (ND Cal 2020) (providing an injunction for WeChat) [hereinafter *WeChat v Trump*].

10 Exec Order No 14034, 86 Fed Reg 31423 (June 9 2021).

11 Special Counsel Robert S Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (2019) 20 <https://www.justice.gov/storage/report.pdf.> accessed 18 April 2021.

counter the spread of "digital barriers" that block access to information. Solutions blocking foreign technology from use within the US undermine the notion of the Internet as the borderless medium that the US has sought to preserve. Given the importance of democratic values at the heart of US Internet Freedom foreign policy, these bans diminish the ability of the US to pressure other governments to preserve the free flow of data and could have also more detrimental long-term global impacts.

In this article, we outline and evaluate the motivations of the US's recent moves to erect digital walls, in the context of the broader US policy on Internet Freedom. Since the early days of US missionaries, many US efforts abroad attempted to spread liberal values.[12] The internet was seen as a technological means of spreading the ideas of free speech and democratic values globally, through expanded opportunities for uncensored communication. This overarching goal is in tension with the attempted technology bans, which the Trump Administration justified in court as necessary to protect national security and mitigate Chinese government censorship. And for a country that has worked to prevent the rise of digital walls and counter China's "cyber sovereignty" foreign policy, taking actions that block an avenue for free expression borrow from China's playbook and normalises the Chinese approach to governing the internet over the very "borderless" internet the US has invested in protecting.

Section I provides context on the US's Internet Freedom policy, laying the groundwork for why these technology bans are so antithetical to America's long standing commitment to an open internet.

Section II then assesses the variety of risks that the US government has cited in court cases as justifying the TikTok and WeChat bans. The US's alleged risks fall into four categories: Chinese government access to American consumer data, Chinese government censorship on the platforms, risks to government employees' data and government infrastructure, and the platforms' roles in propagating disinformation campaigns and election interference. Overall, the US government failed to clearly outline sufficient harms arising from each of these threats that would justify banning communications tools. Only the threat of access to government employees' data and military networks is sufficiently narrow.

Section III more broadly examines the tools the US can use to block foreign technology, and how the structure of these tools encourages opacity

---

[12] Walter Russell Mead, *Special Providence: American Foreign Policy and How it Changed the World* (Routledge 2013).

and allows for dangerous policies like technology bans to be passed into law. The President's power through the International Emergency Economic Powers Act (IEEPA) is the easiest avenue for pursuing action against foreign firms through executive orders. Congressional statutes can also be used to implement bans on foreign technology, but are foreclosed from punishing individual companies. The executive and Congress also have the joint power to investigate foreign investment in technology companies using the Committee on Foreign Investment in the US (CFIUS) reviews, which provide more discretionary power to the government. Together, these tools provide broad discretionary, opaque, and flexible powers to the government to ban technology. This raises concerns over the ease with which the executive can advance bans of communication tools as a solution.

Section IV examines the cost of such bans. First, there are significant First Amendment and free speech concerns, and a violation of these laws and norms could be akin to soft censorship. Second, such bans have a significant impact on international relations and policy, including calling into question Internet Freedom and hurting the foundations of the internet—effectively an exemplification of Krasner's organized hypocrisy.[13] Finally, such bans also have the potential to drastically impact policies around data localization and create incentives for foreign governments to retaliate and create their own digital walls. Norms for cyber security are currently being negotiated at the United Nations, where the US and China have proposed dramatically different approaches.[14] By borrowing from China's playbook and raising digital walls when threats to US sovereignty are at stake, the US is legitimizing China's norms—the same norms that it has invested resources in countering.

We conclude that the costs of banning communications tools based on intangible, broad risks are not outweighed by the alleged benefits to national security and privacy that arise from these bans. Such bans also raise serious free speech concerns and are not worth the short-term gains the US hopes to achieve. They also legitimize other democratic governments'—such as India's—banning of foreign technology, creating a permission structure for closing avenues of speech and undermining the very unsiloed, open nature

---

[13] See generally Stephen D Krasner, *Sovereignty: Organized Hypocrisy* (1999).

[14] Duncan B Hollis, 'China and the US Strategic Construction of Cybernorms: The Process is the Product' (*Lawfare*, 11 July 2017) <https://www.lawfareblog.com/china-and-us-strategic-construction-cybernorms-process-product-0> accessed 26 April 2021; Christian Ruhl, Duncan Hollis, Wyatt Hoffman & Tim Maurer, *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads* (Carnegie Endowment for International Peace 2020) <https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110> accessed 26 April 2021.

of the internet. The US government has many far-reaching and broad instruments to counter threats beyond banning the technology, and these tools do not create incentives for transparency. It should use these tools in a manner that focuses on a clear process to evaluate whether the risks mitigated by such technology bans are worth the heavy global costs of diminishing Internet Freedom and potentially inspiring other governments to raise digital walls and affect free speech.

I. The US's Internet Freedom Policy and Technology Bans

Over the last three decades, the US has championed the internet as a medium for extending liberalism further than previously imaginable. US Supreme Court rulings describe the internet as facilitating free expression, noting that "anyone with an internet connection" can become "a town crier with a voice that resonates farther than it could from any soapbox."[15] American foreign policy for the internet attempted to extend the same values that promoted domestic speech abroad, championing a "borderless" medium where new modes of communication are possible across countries. The central idea behind this policy was that governments should take a limited role in the regulation of the internet and instead allow technical experts to make decisions to prevent government interference in the operation of a global communications platform.[16]

At the heart of the US Internet Freedom policy is an effort to prevent the rise of strategies that limit the movement of information to within national boundaries. These "digital walls" can take many forms, but the main form involves governments disrupting the openness of the internet through censorship or impounding data within borders and preventing the free movement of information.[17] US officials designed the Internet Freedom foreign policy to preserve a borderless internet, which would, by definition, resist such nationalistic efforts to blockaccess to information, because of its boundlessness.

---

[15] *Reno v ACLU* 1997 SCC OnLine US SC 82 : 138 L Ed 2d 874 : 521 US 844, 870 (1997).

[16] See, eg, 'Short History of the Internet' (*Internet Society*, February 1993) <https://www.internetsociety.org/internet/history-internet/short-history-of-the-internet> accessed 14 August 2021. The way the internet is governed, through non-profit bodies and groups like ICANN, IETF, IANA (which are all *prima facie* neutral and non-governmental organizations), is the prime example that the US government intended to let the internet govern itself. See, eg , Stuart Minor Benjamin & James B Speta, *Telecommunications Law and Policy* (2015) 537-44.

[17] Jack Goldsmith & Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (2006) 23.

An internet architecture that operated without regard for national borders extended the possibilities for global communication and speech, ensuring that every individual could access information without regard to where they are located.[18] And strategies like China's Great Firewall are exactly the restrictions the US designed its internet foreign policy to avoid.

The first wave of US foreign policy surrounding the internet questioned the ability of governments to implement digital walls, with President Bill Clinton infamously arguing that trying to regulate the internet would be like "trying to nail Jello to the wall."[19] Years later, Secretary of State Hillary Clinton argued that policies that prevent access to information are as repressive as the Berlin Wall: these efforts only serve to divide societies and limit liberalism.[20] The US invested in efforts to aid activists who were attempting to rise up against repressive states, including circumvention tools that could be used to evade censorship.[21] Of course, in addition to normative impulses to extend liberalism, American companies also benefitted immensely from the light regulation of the private sector, allowing technology giants like Facebook and Google to grow and prosper globally.[22] But even the lack of regulation of these companies is in part justified by the government's desire to not govern speech and content on the internet, both at home and abroad.[23]

After the initial laissez-faire, non-governmental approach to letting the internet develop, emerging policies by foreign governments have called into question the vitality of the US's vision of a borderless internet.[24] Governments have responded to digital threats as they have physical threats: by leveraging the tools of territorial sovereignty and the long-standing power of the state to regulate activity within its borders.[25] Although literature has surveyed China's power to bring the internet under national control, even liberal democracies are, by necessity, shifting, acknowledging the need to implement digital border control strategies to address national security concerns. New emerging threats like election interference and online propaganda now motivate democracies to raise digital walls; for example, in the case

---

[18] Joyce (n 3) 493.

[19] 'User Clip: Clinton on Firewall and Jello' (*C-SPAN*, 8 March 2000) <https://www.c-span.org/video/?c4893404/user-clip-clinton-firewall-jello> accessed 24 April 2021.

[20] Clinton (n 5).

[21] See, eg, James Ball, 'Online Tools to Skirt Internet Censorship Overwhelmed by Demand' *The Washington Post* (21 October 2012).

[22] Anupam Chander, 'How Law Made Silicon Valley' (2013) 63 Emory L J 639.

[23] See, eg, Emily Bazelon, 'Free Speech Will Save Our Democracy' *The New York Times* (13 October 2020) <https://www.nytimes.com/2020/10/13/magazine/free-speech.html>.

[24] 'The Internet's New Borders' (*The Economist*, 9 August 2001*)* <https://www.economist.com/leaders/2001/08/09/the-internets-new-borders> accessed 9 August 2021.

[25] Goldsmith & Wu (n 17).

of misinformation, governments seek to preserve the smooth transition of power and trust in elections, or in the case of cybercrime, to prevent attacks on national industries.

On this new frontier, although some governments are slowly shifting slightly towards China's vision of territorial control, the US has held fast to ideas privileging free information flow. For example, the US government decries data localization laws—strategies that impound data within national borders—as harmful to the concept of internet freedom. The government also uses international trade agreements to preserve a zone of free data flows between signatories.[26] Although more democracies are implementing content moderation to address threats of terrorism, the US broadly[27] adheres to the principle that information flows should remain unadulterated by governments. Another example is the US government's eschewing of intermediary liability laws that require platforms to remove illegal content or face sanctions in all instances except in the case of sex trafficking.[28]

In contrast to this history of American policies upholding the free flow of data and speech, a ban on Chinese communication tools flies in the face of Internet Freedom and broader norms of liberalism that privilege free expression and the right to access information regardless of territorial boundaries. The effort constitutes a puzzling attempt by the architect of Internet Freedom to implement policies it has continuously derided abroad, in the process affecting First Amendment rights that prevent the government from making laws that abridge "the freedom of speech, or the press."[29] Although the US has attempted to prevent the rise of digital walls, counterintuitively, it went against decades of attempts to preserve liberalism online. So, what are the motivations for this about-face, and are these rationales credible?

II. Assessing the Legal Justifications for These Technology Bans

Although the US has advocated against foreign efforts to impose digital walls, the government cites characteristics of Chinese technology as threats

[26] Vipal Monga and Telis Demos, 'U.S. Banks Want Freer Flow of Data in Nafta Pact' *The Wall Street Journal* (2 November 2017) <https://www.wsj.com/articles/u-s-banks-want-freer-flow-of-data-in-nafta-pact-1509624001> accessed 9 August 2021.

[27] Even so, this broad policy is often inconsistent, for example, with the PRISM program.

[28] Aja Romano, 'A New Law Intended to Curb Sex Trafficking Threatens the Future of the Internet as We Know it' (*Vox*, 13 April 2018) <https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom> accessed 9 August 2021.

[29] US Const amend I.

damaging enough to national interests to justify banning Chinese communication tools. This section describes the alleged threats the US government has cited *in court and legally* as a rationale for banning Chinese technology, ranging from consumer privacy to preventing China from conducting censorship across borders.[30] We then analyse what kinds of harms these threats bring, and to whom these harms are posed. This assessment is based on five categories of harm central to cybersecurity law: harms to confidentiality, integrity, availability of information, systems, and networks.[31] Each of these harms may be to individuals, companies, or national security.[32] Finally, we assess whether these harms are based on retrospective threats or prospective ones.[33]

We then offer a rough legal estimation of whether the burden of bans based on each threat is worth the risk or liability if each threat materialized, by assessing the risk of an unaddressed remedy and the utility of implementing a remedy—effectively a derivation of the Learned Hand formula the Second Circuit used in *United States v Carroll Towing Co*, but here in the context of cybersecurity.[34] The Learned Hand formula is used to determine whether an act is negligent. Where the burden of adequate precautionary measures (B) is less than the liability or harm arising out of a potential injury (L), multiplied by the probability of that injury (P), the tortfeasor is negligent unless they implement the precautionary measure. The formula, $B < P * L$, amounts to a risk versus utility trade off.[35]

The US's articulated threats fall into two categories: broad concerns about the influence on consumers and the public (such as access to user data and censorship); and specific national security concerns (such as access of federal government users' data, corporate decision making influenced by adversarial nations, and election interference and the creation of disinformation campaigns). Narrower threats are easier to associate with harms and parties affected, whereas broader threats are either hard to verify as extant, or so broad that those threats are no different from threats associated with most

---

[30] We take this legal approach because other justifications offered for these bans are less concrete, less substantiated (if at all), and less relevant when it comes to whether these bans would have ultimately survived the legal system.

[31] Jeff Kosseff, 'Defining Cybersecurity Law' (2018) 103 Iowa L Rev 985, 1010.

[32] ibid.

[33] ibid.

[34] Scott J Shackelford, Andrew A Proia, Brenton Martell & Amanda N Craig, 'Toward a Global Cybersecurity Standard of Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices' (2015) 50 Texas Intl L J 305, 315.

[35] ibid. For the original analysis, see *United States v Carroll Towing Co*, 159 F 2d 169, 173 (2d Cir 1947).

digital technologies. How the US government positions the threat, both in breadth and in the potential harm, shapes whether the benefits of a ban in mitigating the threat outweigh the expense of free speech protections and internet freedom under US law.

Using the Learned Hand approach to assessing legal justifications, our conclusion is that narrowly defined risks indicate acute potential harm, which might be better suited as a rationale that would withstand First Amendment scrutiny. Since the US government has cited only one acute potential harm, there may be other underlying foreign policy concerns that motivate these digital walls, which will be discussed in Section IV.

A. Privacy Concerns in Access to Consumer Data

The US government fears that China will use data collected by apps to surveil American consumers. This fear has been exacerbated by growing suspicion between the US and China, with the US alleging that the Chinese government can use Chinese technology to access American consumer data, which may implicate confidentiality and data integrity, and harm consumers. Nonetheless, given the ambiguous nature of the threat as defined by the government both in court and in executive orders, mitigating such a broad risk to privacy through a technology ban is not worth the consequences to speech and internet freedom.

First, in the executive orders banning TikTok and WeChat, the Trump Administration noted that "India recently banned the use of TikTok and other Chinese mobile applications . . . [asserting] that they were 'stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India.'"[36] More directly, in addressing WeChat, the executive order notes that "WeChat automatically captures vast swaths of information from its users. This data collection threatens to allow the Chinese Communist Party to access Americans' personal and proprietary information."[37]

The government elaborated on these claims in court cases that arose immediately after the executive orders were signed into law. In *TikTok Inc v Trump*, the government alleged that the Chinese government was "building massive databases of Americans' personal information" to "further its intelligence-gathering and to understand more about who to target for espionage,

[36] Exec Order No 13942 (n 7).
[37] Exec Order No 13943 (n 8).

whether electronically or via human recruitment."[38] In *Huawei Techs USA Inc v United States*, the government alleged that Chinese "cyber activity" could lead to the exploitation of American networks which have Chinese telecommunications equipment embedded within them.[39] More broadly, the government also alleges that Chinese government officials embedded in private Chinese technology companies create an opening for these officials to more directly sway the companies into providing the Chinese government access to American consumer data.[40] Even individuals have raised lawsuits in American courts alleging harm from Chinese surveillance through WeChat.[41]

These broad alleged risks implicate issues of data confidentiality and integrity, and this threat is likely real, judging by recent changes in Chinese law that grant the government broad authority to access data. For example, the number of Chinese Communist Party (CCP) members in management positions in a company, combined with laws like the 2017 Chinese National Intelligence Law (which the US alleges allows Chinese authorities to "take control of any China-based firm's facilities and communications equipment")[42] affect whether data remains confidential and whether it remains unaltered by anyone other than the end-users.[43]

Further, Article 14 of the Chinese National Intelligence Law states that national intelligence institutions "may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation."[44] This broad-based authority is not new, and has teeth: Byte Dance, TikTok's parent company, has previously cooperated with the Chinese

---

[38] *TikTok v Trump* (n 9) [8].

[39] *Huawei Techs USA Inc v United States* 440 F Supp 3d 607, 622 (ED Tex 2020) [hereinafter *Huawei v United States*].

[40] *TikTok v Trump* (n 9) *5 (stating the government's allegations that "TikTok's foreign ownership and data collection pose a risk that the Chinese Communist Party can 'access . . . Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.'") See also *Huawei v United States* (n 39) 622 (stating that the government alleges that "large Chinese companies—particularly those 'national champions' prominent in China's 'going out' strategy of overseas expansion—are directly subject to direction by the Chinese Communist Party, to include support for PRC state policies and goals.").

[41] See, eg, *Citizen Power Initiatives for China v Tencent America LLC* Docket No. 21CV375169 (Cal Super Ct 2021).

[42] *TikTok v Trump* (n 9) [9].

[43] ibid.

[44] 'China's Intelligence Law and the Country's Future Intelligence Competitions' (*Government of Canada*, 17 May 2018) <https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html> accessed 18 April 2021.

government in shutting down one of its media platforms, reflecting the power of the National Intelligence Law in its influence over company operations.[45] The US alleges that "[Chinese] laws can compel cooperation from ByteDance, regardless of whether ByteDance's subsidiaries are located outside the territory of [China]," implying that the law impacts foreign-operated companies.[46] But the scope of authority the Chinese law provides is unclear, as is how that authority impacts user data in practice—and thus leaves ambiguous to what extent confidentiality and integrity are implicated.[47]

Recent American policy may also affect the US government's perception of the risk of access to consumer data, and the harms arising from it. The passage of the Clarifying Lawful Use of Overseas Data (CLOUD) Act, which created a mechanism to demand access to data held on servers in foreign territory for the purpose of law enforcement investigations, allows US government warrants to extend beyond US borders.[48] The Snowden disclosures also

---

[45] Jiayang Fan, 'Why China Cracked Down on the Social-Media Giant Bytedance' (*New Yorker*, 19 April 2018) <https://www.newyorker.com/news/daily-comment/why-china-cracked-down-on-the-social-media-giant-bytedance> accessed 18 April 2021.

[46] *TikTok v Trump* (n 9) [8] - [9].

[47] We also note here a tangential threat: the Chinese government's coercion of companies to enforce domestic policies. However, it is hard to tell when these companies' acts abroad are done at the behest of government force, and there is inadequate information to determine whether this threat implicates access to consumer data at all. See nn 45 and 57 (exemplifying Chinese government acts that censor and shape domestic business policy of tech giants and their users). The line between broad corporate policy being shaped by government policy and specific corporate decisions being forced by individual government actors embedded in an organization is hard to discern, given the opacity of decision making within Chinese firms.

The problem is exacerbated when we examine the decisions made by Chinese-owned firms and those that are mostly privately owned. For example, Chinese state-owned companies are often used as a tool of coercion in Chinese foreign policy. Ketian Vivian Zhang, 'Chinese Non-Military Coercion – Tactics and Rationale' (*Brookings*, 22 January 2019) <https://www.brookings.edu/articles/chinese-non-military-coercion-tactics-and-rationale/> accessed 18 April 2019 (noting an incident where a Chinese state-owned company bought a Norwegian hydro company in order to get access to Norwegian expertise in deepwater drilling). But privately-owned companies are more in line with the broad goal of having indigenous companies "be globally competitive," and it is unclear what low-level decisions are enforced by Chinese government officials. ibid.

Despite this opacity, there are still reasons to be concerned: in 2016, 68% of China's private companies had party bodies, as did 70% of foreign enterprises. Richard McGregor, 'How the State Runs Business in China' *The Guardian* (25 July 2019) <https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei> accessed 18 April 2021. While most of these party bodies are used to influence business decisions, it is unclear if such decisions include access to, and therefore harm, US consumer data—or whether another threat, such as censorship, is implicated. ibid.

[48] See, eg, Jennifer Daskal, 'Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues' (2016) 8 J National Security L and Policy 473; Jennifer Daskal, 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0' (2018) 71 Stanford L Rev Online 9–16; Jean Galbraith, 'Congress Enacts the Clarifying Lawful Overseas Use

revealed a sweeping effort to gather and access foreign nationals' information, reflecting a strong signals intelligence apparatus that had the capacity to breach data confidentiality and integrity.[49] Thus, the threat of "access to consumer data" may indicate American discomfort with a Chinese surveillance apparatus similar to that of the US's in reach.[50]

Even assuming the threat of Chinese government access to consumer data is real, it is ambiguous what tangible harms arise from Chinese access to American consumer data. American companies like Facebook and Google gather enormous data profiles of their users, and may also affect data confidentiality and integrity. The US government also routinely accesses consumer data, both through due process[51] and by buying consumer data.[52] Why, and at what point, a foreign company's (and potentially a foreign government's) access to domestic consumer data poses more danger than a congruent access by a local company or the US government are both unclear. Both domestic and foreign companies' access to US data may have national security impacts, given that foreign governments can theoretically force American companies to hand over data. Transparency about the kinds of threats that Chinese companies uniquely pose by accessing American consumer data may provide credibility to the threat of an outright technology ban.

Even assuming the existence of the threat of access to consumer data by the Chinese government in a manner that implicates national security, mitigating this threat using a foreign technology ban would create more costs

---

of Data (CLOUD) Act, Reshaping US Law Governing Cross-Border Access to Data' (2018) 112 American J Intl L 487.

[49] See generally 50 USC § 1881(a), commonly known as Section 702 of the Foreign Intelligence Surveillance Act, for an example of the US government's ability to access foreign consumer data. The relevant procedural mechanism is the FISA court, which holds such surveillance accountable, though there is significant debate—beyond the scope of this paper—about whether these courts actually enforce accountability.

[50] Henry Farrell and Abraham L Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44 International Security 42.

[51] See, eg, Barton Gellman & Ashkan Soltani, 'NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say' *The Washington Post* (30 October 2013) <http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html> accessed 24 April 2021.

[52] See, eg, Byron Tau & Michelle Hackman, 'Federal Agencies Use Cellphone Location Data for Immigration Enforcement' *The Wall Street Journal* (7 February 2020) <https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600> accessed 24 April 2021. See generally 50 USC § 1881(a), commonly known as Section 702 of the Foreign Intelligence Surveillance Act, for an example of the US government's ability to access foreign consumer data. The relevant procedural mechanism is the FISA court, which holds such surveillance accountable, though there is significant debate—beyond the scope of this paper—about whether these courts actually enforce accountability.

(burden, or B in Learned Hand terms) than benefits from prevented harms (P*L). The costs of such an action are massive. First, since it is widely known that the US government occasionally accesses consumer data, and that American companies construct data profiles, foreign governments could use the same cudgel of "access to consumer data" to bar American companies, causing financial harm. Relatedly, other nations (such as India) may find this a useful signal to allege broad and ambiguous threats to raise digital walls, barring not just American and Chinese companies, but companies from other countries that are pretextually adversarial. There are few benefits to balance these significant costs: while the US would prevent one avenue of accessing consumer data in the short run, the Internet has few borders. The Chinese government would not find it difficult to buy American consumer data—as the American government does[53]—or use other mechanisms (like cyberattacks) to access such data, effectively not reducing the harm from this threat. In Learned Hand terms, the burden (B) incurred in implementing a ban is much higher than the (admittedly likely) liability arising from the Chinese government accessing American consumer data.

In sum, "access to consumer data" is a broad and nebulous threat. It implicates *consumer* data confidentiality and integrity. But how that associates with national security, despite Chinese policy changes that increase government access to Chinese company operations, is not outlined in a legally satisfactory way. Even if such a threat exists, the costs of mitigating it using a technology ban outweigh the benefits of curtailing the threat.

B. Foreign Censorship in the US

In addition to threats to consumer data, the US government contends that the CCP could use its influence and legal apparatus to "[censor] content that the [CCP] deems politically sensitive."[54] Such concerns are grounded in truth and implicate data integrity and access to information. The threat of censorship is a prospective threat to consumers and national security. But because allegations of censorship are broad, and the kinds of censorship which tangibly harm American consumers and the government are unclear, the impacts to speech and digital walls outweigh the benefits of fighting censorship through censoring a foreign technology.

US government concerns about censorship have to do with both censorship of the content American users consume and create, as well as the coverage of politically charged foreign policy issues, such as "content concerning

---

[53] ibid.

[54] *TikTok v Trump* (n 9) *5.

protests in Hong Kong and China's treatment of Uyghurs and other Muslim minorities."[55] In addition, the US government is concerned about the "censorship of critiques about the Chinese government," which is effectively propaganda for the Chinese government.[56]

These allegations of censorship are grounded in historical truth. The Chinese government has a history of censorship on the internet, including on apps and websites that are used beyond its borders.[57] Scholars have described extraterritorial instances of censorship and the reach of online policies that extend beyond national boundaries.[58] Also, American firms have been criticized for bending to the will of the Chinese government, affecting users globally. For example, the Chinese government may have pressured Apple to remove HKmap.live, an app that was used to track police activity by pro-democracy protestors in Hong Kong.[59] More subtly, the Chinese government has pressured American airlines to remove references to Taiwan from their websites globally.[60] While such censorship is tied to economic pressure, it nonetheless indicates the Chinese government's approach to speech not just domestically, but globally.

China can also censor speech beyond its borders by demanding that Chinese firms globally remove particular information. American officials claim that TikTok globally implements demands from the Chinese government to scrub inappropriate or illegal content from the platform.[61] Documented accounts

---

[55] *Marland v Trump* 498 F Supp 3d 624 : 2020 US Dist LEXIS 177129 at *7 (ED Pa 2020).

[56] *WeChat v Trump* (n 9) *3-4.

[57] See, eg, Min Jiang, 'Chinese Internet Business and Human Rights' (2016) 1 Business Human Rights J 139 ("Authorities have also cracked down on WeChat, asking it to remove politically 'harmful' posts and accounts."). WeChat, for example, censors users regardless of their geographic location. Eileen Guo, 'Censored by China, under Attack in America: What's Next for WeChat?' (*MIT Technology Review*, 30 October 2020), <https://www.technologyreview.com/2020/10/30/1011450/wechat-censored-china-under-attack-in-america/> accessed 18 April 2021 (noting that "American WeChat users aren't necessarily subject to the same levels of Chinese internet policing" but that "most content is still subject to the Chinese Communist Party's rules").

[58] See, eg, Jennifer Daskal, 'Borders and Bits' (2018) 71 Vanderbilt L Rev 179, 217 n 131 (examining the difficult and nebulous problem of US-based users who are promoting democracy, and being censored, in China); Jennifer Daskal, 'Speech Across Borders' (2019) 105 Virginia L Rev 1605, 1607 (discussing how China opposed big technology companies like Facebook and Twitter from shutting down pro-China propaganda accounts).

[59] Louise Matsakis, 'Apple's Good Intentions Often Stop at China's Borders' (*WIRED*, 17 October 2019), <https://www.wired.com/story/apple-china-censorship-apps-flag/> accessed 18 April 2021.

[60] Sui-Lee Wee, 'Giving in to China, US Airlines Drop Taiwan (in Name at Least)' *The New York Times* (25 July 2018) <https://www.nytimes.com/2018/07/25/business/taiwan-american-airlines-china.html> accessed 18 April 2021.

[61] Drew Harwell & Tony Romm, 'Inside TikTok: A Culture Clash Where US Views about Censorship Often were Overridden by the Chinese Bosses' *The Washington Post* (5

of messages disappearing and users being blocked from accessing WeChat and TikTok have been reported by users who make posts critical of the Chinese government.[62] Both history and American allegations indicate the ability of the Chinese government to impact both American consumer access to data about foreign events as well as the integrity of conversations and data on Chinese apps.

Thus, although the Chinese government's history of censorship on these applications is clear, the US government's allegations leave unsaid the harm to consumers and national security when such data integrity and access to information is impacted. This is because what constitutes censorship under the US's claims is unclear, especially given that some forms of speech regulation may be considered acceptable censorship. For example, American websites moderate content that users post, including Facebook, Twitter, and Google.[63] While most of this content moderation is not government-mandated, technology companies are liable when users post copyrighted content,[64] hate speech that incites violence,[65] and false advertising,[66] reflecting the government's role in shaping speech online. Without clarification of the harms of censorship, this threat, like Chinese access to consumer data, remains broad and unsophisticated. But such a broad allegation may still be politically credible, since a foreign censor seems far more dangerous than

---

November 2019) <https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/> accessed 18 April 2021 (reporting that "former employees claimed attempts to persuade Chinese teams not to block or penalize certain videos were routinely ignored, out of caution about the Chinese government's restrictions and previous penalties on other ByteDance apps").

62 Jeanne Whalen, 'Chinese Censorship Invades the US via WeChat' *The Washington Post* (7 January 2021) <https://www.washingtonpost.com/technology/2021/01/07/wechat-censorship-china-us-ban/> accessed 18 April 2021; See also Amanda Aronczyk, 'Nervous TikTok' (*National Public Radio* 13 January 2021) <https://www.npr.org/2021/01/13/956558906/nervous-tiktok> accessed 18 April 2021 (starting at 8:14, discussing instances where TikTok videos describing Chinese treatment of Uighurs were "shadow banned," and the creators of these videos had their accounts suspended).

63 See, eg, Kate Conger, 'Facebook, Google and Twitter C.E.O.s Return to Washington to Defend their Content Moderation' *The New York Times* (28 October 2020) <https://www.nytimes.com/2020/10/28/technology/facebook-google-and-twitter-ceos-return-to-washington-to-defend-their-content-moderation.html> accessed 18 April 2021.

64 See, eg, the Digital Millennium Copyright Act, which requires that internet companies block access to material that infringes on copyright, in exchange for liability protection. Pub L No 105-304 112 Stat 2860 (Oct 28 1998).

65 See, eg, *Elonis v United States* 192 L Ed 2d 1 : 575 US ___ (2015) (finding that in order to hold the plaintiff liable for threatening statements made about his ex-wife on Facebook, the plaintiff would have had to have the right *mens rea* or intent to harm the wife).

66 See, eg, *Casper Sleep Inc v Mitcham* 204 F Supp 3d 632, 640 (SDNY 2016) (a case between an online mattress retailer and an online mattress reviewer, who falsely advertised his impartiality of mattress reviews).

domestic regulation of speech, much of which seems either reasonable or within control.

Even so, the use of "censorship" as a threat that justifies banning a foreign technology may create significant consequences (burden, or B in Learned Hand terms) that outweigh the escaped liability (P*L) of preventing some censorship. First, the broad threat of censorship could set precedent allowing the government to ban other apps where foreign governments play a role in regulating American users' speech, but do not *prima facie* censor speech. For example, the German government outlaws the "use of symbols of unconstitutional organizations" like the Nazi party, outside of the contexts of "art or science, research, or teaching."[67] If the German government prevented a German citizen from talking about the Nazi party with an American person, using a German app, that could be painted as censorship.[68] Second, as with access to consumer data, such a threat/action pair could bring scrutiny to American practices of content moderation and self-regulation, with foreign governments chafing at the US government's definition of what constitutes acceptable censorship (i.e. content moderation). This could lead to foreign governments pressuring American companies to follow a content moderation regime in line with the foreign government's values. Finally, by banning technologies, the US risks leaving in dark those users in China and elsewhere who could still communicate with American users and read messages that escape censorship. The soft power of communication—both through messages received and open channels of communication—is inherently undervalued.

These costs—the Learned Hand formula's burden—are not outweighed by the value of the prevented liability, even if it is all but certain that the Chinese government is engaging in online censorship through these apps. For one, the amount of censorship that is currently taking place seems low compared to the value brought in having some access to communication with more than a billion users. By banning apps, the US government is doing the Chinese government's work by strengthening the bubble in which Chinese citizens live. A ban raises the burden, B, incurred by the US, by strengthening Chinese censorship. Further, the CCP's current controlled information

---

[67] 'Strafgesetzbuch § 86a' (*German Law Archive*, 13 November 1998) <https://germanlawarchive.iuscomp.org/?p=752> accessed 18 April 2021.

[68] Especially, as it stands, speech about Nazis, even in the public arena, is considered protected by the First Amendment. See, eg, *National Socialist Party of America v Village of Skokie* 1977 SCC OnLine US SC 113 : 53 L Ed 2d 96 : 432 US 43 (1977) (reversing an Illinois state court's decision to provide an injunction against the NSPA's (a neo-Nazi organization) request for a permit to march in Skokie, reasoning that the display of Nazi logos were not fighting words that were not protected by the First Amendment).

ecosystem is already frowned upon globally. A ban would indicate that the US government is comfortable with controlling the information ecosystem at home, legitimizing the Chinese policy (and perhaps encouraging other countries adversarial to China, like India, to enact their own technology bans), instead of the status quo.

Thus, the idea of "censorship" as a threat is broad and nebulous. It implicates consumer data integrity and access to information, and may tangentially impact national security. Yet, how substantial this threat is, given the undefined contours of "censorship," is unclear. These uncertainties indicate that the small benefit of preventing Chinese censorship by banning Chinese technology may not be worth the costs of retaliation, scrutiny, and loss of communication with foreign users.

C. Risks to US Military and Government Employees

All governments are animated by a desire to protect national security. An explicit and tangible risk to US national security, as opposed to a general threat to consumers, is the potential for the Chinese government to access federal employees' data and disrupt government infrastructure. The history of Chinese cyberattacks on US government data indicates that this risk to government systems and networks has significant harms to national security, and warrants some policy response.

President Trump's Executive Order 13,942 found that TikTok's data collection could allow "China to track the locations of Federal employees and contractors [and] build dossiers of personal information for blackmail."[69] In addition, the government claims that its networks "face significant information security risks, including the threat of unauthorized access, use, disclosure, disruption, modification, or destruction of government information" and that "the development of Internet of Things (IoT) is placing these government networks further at risk" from technology companies stationed in adversarial countries.[70] The National Security Agency (NSA), among other intelligence agencies, has already stated that Chinese "state-sponsored cyber actors . . . exploit computer networks of interest that hold . . . political and military information."[71]

---

[69] Exec Order No 13942 (n 7).

[70] *Huawei v United States* (n 39) 640.

[71] National Security Agency, 'Cybersecurity Advisory' (*US Department of Defense*, October 2020) <https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF> accessed 18 April 2021.

This risk is serious enough that the federal government has taken steps in the past to prevent foreign software and hardware from being used by government employees and on government networks. The government stopped software from Kaspersky Labs (a Russian software company) from being used on its networks, indicating that this perceived risk was due to the connection with Russia.[72] Further, the threat from China is not speculative, given the history of Chinese-origin hacks and attacks towards government workers and agencies. For example, in 2015, the Social Security Numbers (SSNs) and other records of 21.5 million past, present, and prospective federal employees were stolen.[73] While the government did not directly confirm that the Chinese government was behind the attacks, then-Director of National Intelligence James Clapper identified China as the "leading suspect,"[74] and later, a Chinese national was arrested by the FBI in connection with the hacks.[75] Among other attacks are those on the US Navy and its industrial partners.[76] In addition to creating vulnerabilities in infrastructure and defence systems, the information collected could be used for blackmail or to obtain bargaining advantages when the Chinese government possesses sensitive personal information about American officials.

Similarly, Congress also articulated this risk in its CFIUS review of Grindr, the LGBTQ dating app that was previously owned by a Chinese investment firm. CFIUS warned that data collected about American citizens—especially information about sexual preferences or HIV status—could be used to blackmail American officials and military personnel.[77] The review led to

---

[72] 115 PL 91 § 1634 (2017) (prohibiting the use of products and services developed by Kaspersky Lab, a cybersecurity company headquartered in Russia). The language in § 1634 was then effectively reused when banning Huawei products being used on government networks in 115 PL 232, § 889 (2018) (prohibiting the use of "[t]elecommunications equipment produced by Huawei Technologies Company or ZTE Corporation.").

[73] 'Cybersecurity Incidents' (*Cybersecurity Resource Center at US Office of Personnel Management*) <https://www.opm.gov/cybersecurity/cybersecurity-incidents/> accessed 11 November 2021.

[74] Kristin Finklea et al, Cong Rsch Serv, R44111, Cyber Intrusion into US Office of Personnel Management: In Brief (2015) <https://fas.org/sgp/crs/natsec/R441

[75] Devlin Barrett, 'Chinese National Arrested for Allegedly Using Malware Linked to OPM Hack' *The Washington Post* (24 August 2017) <https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html> accessed 18 April 2021.

[76] Gordon Lubold & Dustin Volz, 'Navy, Industry Partners are 'Under Cyber Siege' by Chinese Hackers, Review Asserts' *The Wall Street Journal* (12 March 2019) <https://www.wsj.com/articles/navy-industry-partners-are-under-cyber-siege-review-asserts-11552415553> accessed 18 April 2021.

[77] David E Sanger, 'Grindr is Owned by a Chinese Firm, and the U.S. is Trying to Force it to Sell' *The New York Times* (28 March 2019) <https://www.nytimes.com/2019/03/28/us/politics/grindr-china-national-security.html> accessed 18 April 2021; See also James Fontanella-Khan & Yuan Yang, 'Grindr Sold by Chinese Owner After US National Security

the company agreeing to limit transfers of data to China and basing its headquarters in the US.[78]

Unlike the previous two harms, harms to government employees and infrastructure are narrow and well defined, and in light of the history of Chinese and foreign cyberattacks against US government infrastructure, clearly impact national security. Of course, not all national security threats justify passing policies that may affect civil liberties. The policy response should depend on the nature of the threat. One framework for categorizing these threats is to determine whether they are non-significant, significant, or an act of war.[79] This categorization depends on the "actual and anticipated effects of any cyber incident, including injury, damage, and death."[80] At the very least, prior Chinese cyber-attacks are not non-significant, since they have resulted in significant data theft,[81] the theft of intellectual property,[82] and the risk of damage to physical infrastructure.[83] The kind of threat the US government is alleging is rooted in reality, and not the sort of edge case that is difficult to pinpoint, unlike generalized harms arising from access to consumer data or nebulous notions of censorship. This kind of threat justifies some response.

Concerns' *Financial Times* (7 March 2020) <https://www.ft.com/content/a32a740a-5fb3-11ea-8033-fa40a0d65a98> accessed 18 April 2021.

78 ibid; See also CFIUS discussion, s III.C.

79 Nicole Softness, 'How Should the U.S. Respond to a Russian Cyber Attack', (2017) 12 Yale J Intl Affairs 99, 106.

80 ibid 107.

81 See, eg, Ryan Lucas 'Chinese Hackers Charged in Alleged Cyber-Theft of 145 Million Americans' Data' (*NPR*, 10 February 2020) <https://www.npr.org/2020/02/10/804501991/chinese-hackers-charged-in-alleged-cyber-theft-of-145-million-americans-data> accessed 18 April 2021.

82 See, eg, Jeffrey B Jones, 'Confronting China's Efforts to Steal Defense Information' (*Belfer Center for Science and International Affairs, Harvard Kennedy School*, 2020) <https://www.belfercenter.org/sites/default/files/2020-05/ChinaStealing.pdf> accessed 18 April 2021 (noting that Chinese theft of intellectual property "is costing industry in the range of $180 billion to as high as $540 billion per year" due to cyber espionage). See also Erica D Borghard & Shawn W Lonergan, 'Chinese Hackers are Stealing US Defense Secrets: Here is How to Stop Them' (*Council on Foreign Relations*, 11 March 2019) <https://www.cfr.org/blog/chinese-hackers-are-stealing-us-defense-secrets-here-how-stop-them> accessed 18 April 2021.

83 See, eg, Adam Clark Estes, 'Chinese Army Hackers are Trying to Bring Down US Infrastructure, After All' (*The Atlantic*, 18 February 2013) <https://www.theatlantic.com/international/archive/2013/02/chinese-army-hackers-are-trying-bring-down-us-infrastructure-after-all/318215/> accessed 18 April 2021; Kim Zetter, 'Solar Winds Hack Infected Critical Infrastructure, Including Power Industry' (*The Intercept*, 24 December 2020) <https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/> accessed 18 April 2021; David E Sanger, Julian E Barnes & Nicole Perlroth, 'Preparing for Retaliation Against Russia, US Confronts Hacking by China' *The New York Times* (7 March 2021) <https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html> accessed 18 April 2021.

However, responding to the threat to government systems and networks through a technology ban may not be worth the costs to speech and internet freedom. The burden B, or cost in the Learned Hand formula, is one to civil liberties. Assessing the value of this burden is entirely subjective, and therefore difficult to estimate.[84] But US courts and the government are generally comfortable with abridging civil liberties—especially those related to the First Amendment—during wartime or when serious national security risks are involved. For example, in *Schenck v United States*, the Supreme Court upheld a statute that ambiguously forbade speech "advising or teaching the duty . . . or propriety of overthrowing" the government.[85] More recently, in *Holder v Humanitarian Law Project*, the Court upheld provisions of the Material Support Statute, which forbade Americans from providing legal services or even advocacy training to any organization the State Department designated as a terrorist organization—including, controversially, the Kurdistan People's Party.[86] The Court has also upheld the Patriot Act, which allows for surveillance of non-US persons when related to national security.[87] Beyond the First Amendment, the Court has upheld bans on movement and immigration during wartime, first in *Korematsu v United States* (where the Court upheld forced internment of Japanese-American citizens),[88] and recently in *Trump v Hawaii* (where the Court upheld the travel ban against some Muslim countries).[89] In short, in scenarios such as US-China cyber hostilities, civil rights may not be valued highly by courts.

On the other side of the Learned Hand equation is the liability and probability of harm (P*L). The probability of a cyberattack that leverages data or application infrastructure is not insignificant, given the escalating pattern of Chinese cyberattacks. The liability, or cost of harms, is high, ranging from intellectual property theft to damage to critical infrastructure. Even assuming the abstract harm to civil rights is high, the cost on the other side is likely higher, given the risk of damage and death arising from escalating cyberattacks. Simply put: the risk to government employees and infrastructure is real, and the harms avoided *may* outweigh the costs to civil liberties.

---

[84] In fact, courts are hesitant to provide compensatory damages in § 1983 claims (generally claims where the government violates constitutional rights and plaintiffs sue the government), where the award focuses on the abstract value of the constitutional right at issue. See, eg, *Memphis Community School Distt v Stachura* 1986 SCC OnLine US SC 148 : 91 L Ed 2d 249 : 477 US 299, 308 (1986) (noting that "the abstract value of a constitutional right may not form the basis for § 1983 damages").

[85] 1919 SCC OnLine US SC 62 : 63 L Ed 470 : 249 US 47 (1919).

[86] *Holder v Humanitarian Law Project* 2010 SCC OnLine US SC 75 : 561 US 1, 9-10 (2010).

[87] See, eg, Susan N Herman, 'The USA Patriot Act and the Submajoritarian Fourth Amendment' (2006) 41 Harvard Civil Rights-Civil Liberties L Rev 67, 78.

[88] 1944 SCC OnLine US SC 135 : 89 L Ed 194 : 323 US 214 (1944).

[89] 138 S Ct 2392 : 585 US __ (2018).

Even with this close calculus, a narrower approach to securing government networks may be more beneficial in the long run. Especially given limited political capital and the difficulty of a systemic approach to improving government cybersecurity, a ban on foreign technology could be passed in lieu of improving government cybersecurity infrastructure, leaving vulnerabilities such as those that led to the latest Russian hacking of US government systems unaddressed.[90] There is also incentive to develop a more targeted remedy: if the government articulates the risk of a foreign technology this narrowly, remedies that impact speech will likely have to be as narrowly-tailored as possible, so as to minimally infringe upon First Amendment rights of users.[91] Finally, while the Court has been amenable to abridging civil rights during wartime, setting a precedent, through a technology ban, of policy that abridges an avenue of speech is a dangerous path, and one that should be trod upon only when other options are exhausted.

To sum up, the threat to government workers and infrastructure is a clearly articulated threat that falls neatly within the framework of cybersecurity law, impacting systems and networks. This clearly implicates national security, and the threat is substantial—and perhaps the costs of such a threat are higher than the burdens on civil liberties. But, while addressing such risks through a technology ban may well be worth some cost to speech and internet freedoms, there are better ways of mitigating such a risk that provide more protections to speech and civil rights.

D. Chinese Election Interference and Disinformation Campaigns

Finally, the US government contends that there is a risk "of disinformation campaigns that benefit the [Chinese government], such as when TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus."[92] Both Democratic and Republican elected officials have also expressed concern that TikTok is a "potential target of foreign influence campaigns, like those carried out during the 2016 election." This indicates that disinformation campaigns pertaining to elections may be a risk incurred due to the use of TikTok.[93] Such risks implicate data integrity and access

---

[90] David E Sanger, Nicole Perlroth & Julian E Barnes, 'As Understanding of Russian Hacking Grows, So Does Alarm' *The New York Times* (2 January 2021) <https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html> accessed 18 April 2021.

[91] See s IV.A

[92] *TikTok v Trump* (n 9) 5.

[93] 'Letter from Charles E. Schumer and Tom Cotton to Joseph Maguire' (*United States Senate*, 23 October 2019) <https://www.democrats.senate.gov/imo/media/doc/10232019%20TikTok%20Letter%20-%20FINAL%20PDF.pdf> accessed 18 April 2021.

to information, in a manner that prospectively impacts national security. But evidence of the Chinese government engaging in election interference is scant. Evidence of Chinese disinformation campaigns is part reality, part myth.[94] And the harm from such campaigns has only begun to be realized. Like the threat of censorship, without a clear understanding of what kinds of election interference and disinformation are being propagated, it is impossible to assess the actual dangers to national security, and difficult to understand whether a technology ban is the most effective approach, or at least one worth the costs to free speech and internet freedom.

Admittedly, social media platforms are vessels for propagating disinformation and exacerbating election interference campaigns.[95] The Russian government used Facebook, Twitter, YouTube, and Instagram in its 2016 election interference campaign.[96] Also, in the 2020 election, Facebook and Twitter, among others, have been in the spotlight for the intensity and volume of disinformation—especially pertaining to elections—that courses through their networks.[97] Given this, it is possible that TikTok, as a major social media platform in the lead-up to the 2020 election, was a vessel for disinformation. However, the extent to which the Chinese government used the platform to impact the 2020 election is unclear, especially at the time of writing. Additionally, the primary source of election interference in 2016 was Russia, and the Mueller Probe and Congress took significant steps to uncover proof of this interference. In contrast, claims about Chinese interference in American elections through a disinformation campaign are unsubstantiated or even decried, and proof about such interference is unlikely to be forthcoming without such an investigation.[98] Nonetheless, the broad

---

[94] Dustin Volz, 'U.S. National Security Adviser Says China Targeting 2020 Election' (*The Wall Street Journal,* 9 August 2020) <https://www.wsj.com/articles/u-s-national-security-adviser-says-china-targeting-2020-election-11597007831> accessed 9 August 2021. Note that "Mr O'Brien's comments were met with skepticism by other officials familiar with the matter. While China has an active interest in the election, the U.S. doesn't currently have intelligence showing that Beijing is directly trying to hack election-related systems, the officials said."

[95] Hunt Allcott & Matthew Gentzkow, 'Social Media and Fake News in the 2016 Election' (2017) 31 J Econ Persp 211, 212 (discussing that "the most popular fake news stories were more widely shared on Facebook than the most popular mainstream news stories" and that "115 pro-Trump fake stories . . . were shared on Facebook a total of 30 million times").

[96] See generally Select Committee on Intelligence, US Senate, *(U) Report* (Vol 2, Committee Print 2020) <https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf> accessed 18 April 2021.

[97] Alex Webb, 'Disinformation Threatens Other Elections After US Voting Ends' *Bloomberg* (3 November 2020) <https://www.bloomberg.com/news/articles/2020-11-03/election-2020-disinformation-on-facebook-twitter-looms-after-polls-close> accessed 18 April 2021 (discussing that "disinformation, propaganda, and fake news are as big a problem elsewhere as they are in the US" on Facebook, Twitter, and Alphabet).

[98] Volz (n 94).

allegation that TikTok *could* be used to sow disinformation and impact elections likely implicates data integrity and access to information, but only because TikTok is just another social media platform where disinformation and election interference are common occurrences.

There is also some truth to the allegation that TikTok plays a role in spreading disinformation—as does all social media. However, the threat of disinformation spread is broad, and the threshold for the kinds and amounts of disinformation that threatens data integrity and access to information in a manner that harms national security has not been clearly articulated by the government. A significant amount of Russian government-backed disinformation (amongst others) flows through Facebook, Twitter, and other American companies. Yet, the government has not taken steps towards curbing disinformation on domestic platforms, indicating that some amount of disinformation may be acceptable and not worth disrupting, given the-side-effect of affecting speech and other civil liberties.

Even assuming that the threat of Chinese disinformation and election interference exists in a well-articulated, clear form, the costs (B) of addressing this threat are not worth the prevented liability (P*L). Without a clear rule about how disinformation on TikTok is more harmful than those on domestic platforms and what harms must be mitigated, the US government opens American platforms to retaliation in foreign countries. Further, a foreign technology ban because of disinformation originating from China will not stop Chinese disinformation campaigns from permeating domestic platforms, without parallel regulation of domestic companies like Facebook and Twitter. Instead, such a technology ban may have the perverse consequence of reallocating disinformation resources to Facebook and other social media platforms that have larger user bases than TikTok, increasing the strength of these foreign campaigns.

In sum, there is some evidence of Chinese disinformation campaigns, but little to none of the Chinese election interference. Nonetheless, the American government's articulation of this threat is not well defined. While the threat impacts data integrity and access to information in the context of national security, the magnitude of this threat is unclear. The little benefit of mitigating this threat through a foreign technology ban is not worth the cost of shifting disinformation onto more widely-used platforms like Facebook.

III. The Methods of Raising Digital Walls in the US

Given that the US has framed the issue as a threat to security interests and sovereignty, there is a broad array of tools at the government's disposal. To combat the aforementioned risks posed by foreign technology companies, the US government has used three main tools:[99] the IEEPA, which is used by the President to handle threats that may cause national emergencies; Congressional statutes that can protect privacy by preemptively imposing sanctions on companies that may cause harm; and CFIUS review, which is a tool jointly employed by the President and Congress to investigate foreign investments in technology companies. Together, these tools give the executive and the legislature broad power, albeit subject to some constraints, to act against technology companies, even if the risks are not yet rooted in reality. We provide a brief overview of these tools and assess the broader structural problem: that such blunt, powerful tools create incentives to enact such technology bans, even at the expense of civil liberties and undermining existing US Internet Freedom policy.

A. IEEPA

IEEPA authorizes the President to approach "unusual and extraordinary threat[s] . . . . to the national security, foreign policy, or economy of the United States" that originate from outside the US, by allowing the President to declare a national emergency regarding that threat.[100] Concerning foreign companies like TikTok, the Act authorizes the President to "investigate . . . , regulate . . . , or prohibit . . . transactions involving any property in which any foreign country or a national thereof has any interest . . . subject to the jurisdiction of the United States . . . ."[101] However, the act forbids the President from exercising such authority over "any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value. . .", or "the importation from any country . . . of any information or informational materials, including . . . news wire feeds."[102] Finally, the IEEPA also grants broad authority to the President when dealing with economic or industrial espionage occuring in cyberspace, allowing the President to "block and prohibit all transactions in all property and interests

[99] This list is not a comprehensive one, but only outlines the main tools that fit within the limited scope of this paper.
[100] 50 USC § 1701(a).
[101] 50 USC § 1702(a)(1)(B).
[102] 50 USC § 1702(b)(3).

in property" against *persons* who are engaging in economic or industrial espionage in cyberspace of intellectual property of US persons.[103]

Thus, the IEEPA effectively grants the President a strong, albeit conditional, power to regulate foreign corporations that pose a danger to the US, but creates exceptions for personal communications technologies. Presidents Trump and Obama have exercised the authority accorded to them by the IEEPA thrice to address cybersecurity threats stemming from Chinese companies. President Obama signed Executive Order 13,694 to target persons engaging in "malicious cyber-enabled activities" through sanctions, including individuals who use computers to harm critical infrastructure, cause a disruption to the internet, or conduct online theft.[104] President Trump then signed Executive Order 13,848, which sanctions individuals conducting foreign interference in the US elections by "materially assisting . . . or providing technological support . . . ."[105] It also allows the executive branch to exclude a company's alien corporate officers from the US.[106] Finally, the most prominent Executive Order is 13,873, which addresses securing information and communications technology and services by allowing the executive branch to prohibit the transfer or installation of foreign technologies that pose a threat to national security.[107] This final order was the basis for the Executive Orders issued to address threats posed by TikTok[108] and WeChat.[109]

Taken together, the IEEPA enables the President, who acts alone through executive orders, to target individuals and companies known to be maliciously impacting the US through communication technologies. However, the President must first declare a national emergency before he can exercise authority under the IEEPA.[110] Additionally—and most importantly—the President cannot regulate personal communications or informational materials.[111]

Despite these minor controls, the wording of the three aforementioned Executive Orders indicates that this tool can have a broad scope, and at

---

[103] 50 USC § 1708(b).
[104] Exec Order No 13694, 80 Fed Reg 18077 (Apr 1 2015).
[105] Exec Order No 13848, 83 Fed Reg 46843 (Sept 14 2018).
[106] ibid.
[107] Exec Order No 13873, 84 Fed Reg 22689 (May 17 2019).
[108] Exec Order No 13942 (n 7).
[109] Exec Order No 13943 (n 8).
[110] *Marland v Trump* (n 55) 13.
[111] ibid. In at least one other case, the courts have specifically prevented the President from regulating communications apps because the President is not allowed to regulate "personal communication[s]." *United States Wechat Users Alliance v Trump* 20-cv-05910-LB 2020 US Dist LEXIS 197776 at 3-4 (ND Cal 2020).

the least can be used to hamper the operations of foreign companies on US soil, without the President having to truly articulate and "prove" in court the risks to privacy and national security. This means there is little incentive to elaborate on how the privacy concerns pertaining to consumer data, censorship, and disinformation campaigns mentioned are tied to national security. Further, since cyberattacks are often unattributable, and can use technology without the consent of the user (e.g. through a Distributed Denial of Service attack), Executive Orders provide the flexibility to sanction individuals who may be indirectly or vaguely associated with attacks, under the guise of national security.[112] Finally, and most critically, IEEPA's breadth creates a structure for the President to "prohibit" technology,[113] rather than take the narrower approach of addressing the underlying risks. For example, since IEEPA can be used to ban technology—and can be done unilaterally by the executive—it may be an easier solution than more targeted solutions that protect consumer privacy or prevent disinformation.

B. Congressional Statutes

The legislative branch also has considerable power in this arena: Congress can pass legislation that targets corporations that it considers a threat to national security. However, Congress cannot pass bills that specifically punish a single entity, known as bills of attainder.[114] Statutes that legislatively determine guilt, whether retrospective or prospective, are considered invalid.[115] Courts look at whether statutes are a legitimate regulation of conduct, which is allowed; or whether they are punishment, which is prohibited.[116]

---

[112] Attribution is difficult because "[c]omputer networks are not designed to facilitate attribution, and hostile actors exploit this weakness to hide their true identity." Eric F Mejia, 'Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework' (2014) 8 Strategic Studies Q 114, 121-22.This can be done through a variety of methods, including spoofing, host laundering, and attacks spread over months. ibid. Attribution is further complicated if attackers use methods like a Distributed Denial of Service Attack (DDoS), which use networks of bots—hijacked computers that, unknown to the user, are involved in malicious attacks—to shut down websites or online services. See, eg, Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) 30 Berkeley J Intl L 525, 555-56. Because the laws of international relations and war, and the laws of cyberspace are so orthogonal, it seems almost impossible to identify persons engaging in "malicious cyber-enabled activities" or providing "technological support" for election interference.

[113] 50 USC § 1702(a)(1)(B).

[114] US Const art I, § 9, cl 3. See also *Nixon v Administrator of General Services* 1977 SCC OnLine US SC 152 : 53 L Ed 2d 867 : 433 US 425, 476 (1977) (noting that retrospective statutes include those that "[inflict] deprivations on some blameworthy or tainted individual in order to prevent . . . future misconduct.").

[115] *United States v Brown* 1965 SCC OnLine US SC 123 : 14 L Ed 2d 484 : 381 US 437, 458-59 (1965).

[116] *Nixon*, 1977 SCC OnLine US SC 152 : 53 L Ed 2d 867 : 433 US 425, 476 (n 114).

Even so, statutes which target a single company can still be legitimate if there are "legitimate justification[s]."[117]

An example of a legitimate statute is the 2019 National Defense Authorization Act, which prohibited regulatory and government agencies from procuring telecommunications equipment from Chinese companies Huawei, ZTE, Hytera Communications, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company.[118] The statute was ruled to be constitutional because the government had the nonpunitive purpose of securing "the federal government's information systems," which included protecting the government's networks from the risk of Internet of Things (IoT) devices.[119] China's history of attacking government networks, including through private contractors, provided a rationalization for such a risk.[120] A similar risk from Russian government cyberattacks was used as justification for prohibiting the use of Kaspersky Lab products by the American government.[121] Note however in both these cases that Congress only limited the *federal government* from using or purchasing the selected companies' products, and did not prohibit private citizens from buying from these companies.

Put simply, Congress can target companies it considers risky, especially if there is a history of attacks originating from the countries of origin. However, the noted limitations—nonpunitive actions and the need for legitimate justification—effectively require Congress to provide well-articulated risks, *unlike* the ones in Section II, before implementing technology bans and raising digital walls. And the limitations and statutory precedent indicate a preference for narrower policy solutions, like preventing the federal government from buying foreign technology, rather than an all-inclusive ban. But history may not be an indicator of the future. Given Congress' broad statutory power,[122] especially in the realm of national security, and given the established risks in the domain of cyberspace, Congress may chart a new path forward and engage in broader technology bans. But given the cumbersome

---

[117] ibid 472 & 477.

[118] John S McCain National Defense Authorization Act for Fiscal Year 2019 § 889 PL 115-232 (2018).

[119] *Huawei v United States* (n 39) 639-40.

[120] ibid 641. This history of attacks is also what lends legitimacy to the risk to federal employees and government infrastructure that the government has articulated in the TikTok and WeChat bans, noted in s II.C.

[121] National Defense Authorization Act for Fiscal Year 2018 § 1634 PL 115-91 (2017). See also *Kaspersky Lab Inc v United States Department of Homeland Security* 909 F 3d 445 (DDC 2018) (upholding the restriction under *Nixon* and finding that the targeting of Kaspersky products was not a violation of the bill of attainder clause).

[122] See, eg, US Const art I, § 8, cls 10-16.

nature of Congressional action, combined with Congressional gridlock, statutory action is the least likely of the three, even though it is the one that creates the most precedent and potential for narrow policy approaches.

C. CFIUS Review

The Congressional Committee on Foreign Investment in the US, or CFIUS, conducts reviews that focus on the national security implications of foreign investments in American companies or operations. The committee's focus is on ensuring that American technology is not transferred to countries that pose national security risks, as opposed to focusing on day-to-day operational decisions made by companies.[123] Broadly, CFIUS reviews look at transactions where a foreign government has a "substantial interest," and then the committee conducts national security risk assessments and creates potential protective measures to prevent impacts to national security.[124] The review's scope has recently expanded with the Foreign Investment Risk Review Modernization Act of 2018, which allows for CFIUS review to focus on "critical technolog[ies]" and "critical infrastructure."[125] The act also focuses on Chinese investment in the US.[126] Generally, however, the CFIUS review is "highly secretive."[127]

The CFIUS review has been used recently to examine Chinese investment into American hardware and software companies. In 2016, due to national security concerns, President Obama blocked Chinese company Grand Chip Investment from acquiring a controlling interest in the American assets of German company Aixtron, a semiconductor coating manufacturer.[128] This was only the third time a President had used CFIUS review to prevent foreign investment, indicating the extraordinary circumstances and importance of Aixtron's assets in the US.[129] The next time a President used the review

---

[123] Cong Rsch Serv, RL33388, The Committee on Foreign Investment in the United States (CFIUS) 1 (2020).

[124] ibid 14.

[125] ibid 2.

[126] ibid 11.

[127] See, eg, David E Sanger, 'Grindr is Owned by a Chinese Firm, and the US is Trying to Force it to Sell' *The New York Times* (28 March 2019) <https://www.nytimes.com/2019/03/28/us/politics/grindr-china-national-security.html> accessed 19 April 2021 (noting that CFIUS is "a highly secretive panel").

[128] Exec Order Regarding the Proposed Acquisition of a Controlling Interest in Aixtron SE by Grand Chip Investment GMBH 81 Fed Reg 88607 (Dec 2 2016).

[129] The first Presidential use of CFIUS was by President George H.W. Bush, who voided the sale of aircraft parts maker Mamco Manufacturing to a Chinese state-owned aircraft company. The second was by President Obama, who ordered Chinese investors to divest from wind farm projects located near a US Navy Weapons systems training facility. See n 123 at 21.

was in 2017, when President Trump blocked a Chinese investment firm from acquiring Lattice Semiconductor, again for national security concerns.[130] However, national security concerns are not limited to China; in 2018, President Trump blocked the acquisition of Qualcomm, a semiconductor maker, by Broadcom, which is based in Singapore.[131]

And, presidential action is not needed to prevent foreign investment into domestic companies. In 2019, Congress initiated a CFIUS review of Chinese firm Beijing Kunlun Tech's acquisition of Grindr, the popular LGBTQ dating app. The review may have been triggered by access to US officials and government contractors' app data, including users' location data,[132] and the review caused the Chinese firm to divest itself of the app.[133] A similar concern over data privacy caused CFIUS to block a merger between MoneyGram, a money transfer company, and Ant Financial, a Chinese e-payments company.[134]

While secretive, the history of CFIUS review and presidential orders using CFIUS review indicates that Congress and the Executive find the review an easy, opaque, and effective method of blocking the sale of companies that may be of national security concern. The use of the review in the past decade indicates that the sale of American technology companies to Chinese or China-proximate companies could pose a national security concern, but does not provide insight into what risk specifically, beyond the vague notion of "access to personal data," exists. This is problematic, especially if policymakers and lawyers want to shed light on the reasoning behind American motivations for digital walls. On the other hand, CFIUS review (without 'the') is generally used to protect existing companies from receiving foreign investors, rather than outright and proactive bans. Thus, the use of this tool may be to indirectly prevent the growth of home-grown technologies, rather than preventing foreign companies from establishing or continuing a US presence. Still, this subtle form of creating an "investment wall" is an extension of digital walls, and the lack of process transparency is troubling.

---

[130] Exec Order Regarding the Proposed Acquisition of Lattice Semiconductor Corporation by China Venture Capital Fund Corporation Limited 82 Fed Reg 43665 (Sept 13 2017).

[131] Exec Order Regarding the Proposed Takeover of Qualcomm Incorporated by Broadcom Limited 83 Fed Reg 11631 (Mar 12 2018).

[132] Sarah Bauerle Danzman & Geoffrey Gertz, 'Why is the US Forcing a Chinese Company to Sell the Gay Dating App Grindr?' *The Washington Post* (3 April 2019) <https://www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr/?utm_term=.799ee5be1f32> accessed 19 April 2021.

[133] ibid.

[134] Ana Swanson & Paul Mozur, 'MoneyGram and Ant Financial Call Off Merger, Citing Regulatory Concerns' *The New York Times* (2 January 2018) <https://www.nytimes.com/2018/01/02/business/moneygram-ant-financial-china-cfius.html> accessed 19 April 2021.

IV. The Implications of Digital Walls

Questions of borders and digital walls implicate free speech, both domestically and globally.[135] US internet users will be denied a communication platform, which may have implications concerning the First Amendment. Additionally, global implications that must be considered include how such technology bans will undermine the US Internet Freedom policy and how such bans may undermine the borderless technical foundations of the internet, lending support for the Chinese vision of the internet.

A. First Amendment and Free Speech

If the government aims to ban apps entirely, as in the case of WeChat and TikTok, courts may consider the consequences relating to the First Amendment implications. The First Amendment prevents the government from making laws that "[abridge] the freedom of speech, or that of the press."[136] Banning apps like WeChat that serve as "public square[s]"[137] raise First Amendment concerns, and the government must satisfy heightened scrutiny for the ban to be upheld by courts. In court, this requires assessing whether the abridgement of speech is narrow enough and sufficiently justified by government need. Where a law regulates speech in a content-neutral manner, the government must satisfy some requirements of intermediate scrutiny i.e., the law must be "(1) narrowly tailored, (2) serve a significant governmental interest unrelated to the content of the speech, and (3) leave open adequate channels of communication."[138] When the law regulates speech in a manner that is content-based (i.e. discriminates against a specific viewpoint), strict scrutiny applies.[139] Strict scrutiny requires the government to prove that the restriction "furthers a compelling interest and is narrowly tailored to achieve that interest."[140]

It is unclear whether banning an app is content-neutral or content-based. For example, banning an app is a time, place, and manner restriction that prohibits *all* speech at a given place (the app), and such regulation requires

---

[135] *Who Controls the Internet* (n 17) 150.
[136] US Const amend I.
[137] *WeChat v Trump* (n 9) 26-28.
[138] ibid (citing *Ward v Rock against Racism*, 1989 SCC OnLine US SC 140 : 105 L Ed 2d 661 : 491 US 781, 791 [1989]).
[139] See, eg, *Reed v Town of Gilbert* , 192 L Ed 2d 236 : 576 US 155, 172 (2015).
[140] See, eg, *Ward v Rock against Racism* 1989 SCC OnLine US SC 140 : 105 L Ed 2d 661 : 491 US 781, 791 (1989) ("the government may impose reasonable restrictions on the time, place, or manner of protected speech, provided the restrictions" satisfy intermediate scrutiny).

intermediate scrutiny.[141] At the same time, certain apps have specific types of content, so banning the app could be content-based. For example, WeChat's content focuses on Chinese-language speakers and relays issues and information pertinent to Chinese speakers. Courts have not adequately considered this problem, to determine whether such a ban is content-neutral or content-based. Nonetheless, at minimum, intermediate scrutiny applies—and even this would be hard for the government to satisfy.[142]

The narrowness prong of the test is averse to outright bans on an app, especially where the ban may be incongruent with the government's assessment of potential risk. For example, in *US WeChat Alliance v Trump*, the Trump Administration tried to ban downloads of WeChat due to national security concerns, one of which was that the app was being downloaded on government devices.[143] The court found that "barring WeChat from government devices" is a narrowly tailored alternative to an outright ban, which it did not deem to be sufficiently narrow.[144] Thus, the government's assessment and allegation regarding the risks it faces plays a critical role in determining whether the solution—banning an app—is legally permissible.[145] In the cases assessed in this paper, the risks defined by the government have varied.[146] If the actual risks are to consumer data and censorship, then an app ban, regulation, or changes to the app may be as "narrow" as possible and may fulfil the second prong of the test, i.e., the requirement that the ban must have a significant relation to a governmental interest *unrelated* to the speech itself (in this case, protecting American consumers). However, if the risks

---

[141] ibid.

[142] The picture is further complicated by the question of whether the speech considered is political or commercial. See, eg, *Buckley v Valeo* 1976 SCC OnLine US SC 16 : 46 L Ed 2d 659 : 421 US 1, 25 (1976) (applying strict scrutiny to political speech); *Central Hudson Gas & Electric Corpn v Public Service Commission* 1980 SCC OnLine US SC 139 : 65 L Ed 2d 341 : 447 US 557, 566 (1980) (applying intermediate scrutiny to commercial speech). It is unclear whether an app ban falls in the category of political speech, or of commercial speech, and courts have not conducted adequate analysis on this. See, eg, *TikTok v Trump* (n 9) 26, where the court assesses a ban on WeChat in terms of strict scrutiny.

[143] *WeChat v Trump* (n 9) 28.

[144] ibid.

[145] Note also that courts are deferential to the government's definition of risks, especially in issues about national security. Effectively, the government's narrative in defining the risk might be taken at *prima facie* value. For example, in *Holder v Humanitarian Law Project* 2010 SCC OnLine US SC 75 : 561 US 1, 33-34 (2010) the Court deferred to the government's claims about risks arising from providing designated terrorist organizations legal support, stating that "evaluation of the facts by the Executive, like Congress's assessment, is entitled to deference." See also *Ziglar v Abbasi*, 137 S Ct 1843 : 582 US ___ (2017) where the court noted that the separation of powers prevented the Court from questioning the Executive's decisions in the realm of national security. The Court ruled similarly in *Hernandez v Mesa* 206 L Ed 2d 29 : 140 S Ct 735 589 US_(2020), 740-42 regarding the Executive's role in international law.

[146] See s II.

are primarily to government employees, then a narrowly tailored solution preventing government employees from downloading that app on government devices may be the only permissible one, and the second prong of the test may not even be reached. Either way, since issues concerning election interference, foreign control of apps, and data access are in flux and have not been extensively litigated in the courts, it remains to be seen whether the government could curtail speech in favour of national security.

If the first prong is fulfilled, it is likely that the second prong—significant governmental interest unrelated to the content of the speech—will also be fulfilled. This is because the risks being cited in Section II have to do with national security, election integrity, and the like, which are unrelated to the content of the speech, and directly related to the existence of the app.

The third prong—adequate alternate channels of communication—plays a subtler role. In *WeChat*, the plaintiffs alleged that their app—which is the primary app for Chinese-speaking and Chinese-American users—had no "viable substitute platforms."[147] In WeChat's case, this is true: no other Chinese language communications app has as broad a user base, nor serves as many functions, as WeChat does.[148] However, TikTok, as an app, is less unique and more substitutable, and in pending litigation, courts have not assessed whether banning TikTok would leave open no alternative means of communication.[149]

The specific factors that courts use to define "substitutability" in the context of digital technologies are unclear.[150] Apps and technology companies

---

[147] *WeChat v Trump* (n 9) 27.

[148] See, eg, 'Number of monthly active WeChat users from 2nd quarter 2011 to 3rd quarter 2020' (*Statista*, 1 December 2020) <https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts/https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts> accessed 31 December 2020.

[149] *Marland v Trump* (n 55) 24.

[150] Antitrust law, which provides criteria for which products are substitutable, is unhelpful. In *Brown Shoe Co v United States* 1962 SCC OnLine US SC 114 : 8 L Ed 2d 510 : 370 US 294, 325 (1962), the Supreme Court focused on seven factors, most of which are price-related: (1) industry or public recognition of separate markets; (2) a product's peculiar characteristics and uses; (3) unique production facilities; (4) distinct customers; (5) distinct prices; (6) sensitivity to price changes; and (7) specialized vendors. Unfortunately, in the case of apps which are free, only factors (2) and (4) are relevant here, and indicate that WeChat may not be substitutable. But courts have yet to address substitutability in the context of social media and app-based technology, so looking at antitrust law may not provide adequate guidance, especially given the balancing test-nature of antitrust regulation in this area. See, eg, Wilson C Freeman & Jay B Sykes, Cong RschServ, R45910, Antitrust and "Big Tech" 25-32 (2019) <https://fas.org/sgp/crs/misc/R45910.pdf> accessed 16 August 2021. It becomes even more unclear because where a market is two-sided (e.g. video streaming, where one side is the viewer and the other the producer), the two sides may disagree about whether alternative platforms are substitutable. Erik Hovenkamp, Platform Antitrust

advertise their uniqueness, and depending on the level of granularity, apps and platforms can look distinct or homogenous. Facebook, Twitter, TikTok, Instagram, and Snapchat are all social media platforms. However, the specific features of Instagram—including the ability to send videos and disappearing pictures—make it a feasible substitute for Snapchat. Instagram and Snapchat's video-sharing features may also make them substitutes for TikTok. Yet TikTok's user base and content discovery functions (such as search features and algorithms that power its feed) are different from those offered on Instagram and Snapchat. Which features are considered and how broadly or narrowly a platform's purpose or functionality is defined will impact whether the platform is considered substitutable. Additionally, the size and demographic of the user base may also play a role. If American WeChat users are forced to migrate to another communication app like WhatsApp or Signal, but users in China are unable to use such apps, or those receiving messages are not on the new apps, then the new apps may not be perfect substitutes for the banned app. To sum: even if the ban is narrow and related to a governmental interest, it may not satisfy heightened scrutiny if the ban also does not provide an alternate channel of communication.

Beyond the tests applied to courts, there are other impacts to speech that are concerning. First, temporary injunctions that oscillate based on courts' decisions may have a chilling effect on speech on these platforms. Users may fear that such platforms may not be around for long, causing migration to other platforms, fragmentation of user bases, or cessation of usage altogether. Especially on platforms like TikTok, where users have monetized their presence, uncertainty may reduce the attractiveness of the public forum.[151] If a user's primary viewership, network, or identity is built around one platform, users may be disincentivized from developing content on these platforms if the government can ban, threaten, or slow these apps down in courts. Second, the government could use data privacy, data access, disinformation, and national security as pretexts for banning or curtailing the

---

[2019] 44 J Corp L 713, 730. Here, it is unclear whether WeChat is part of a two-sided market, but it could be: on one side are users who have access to a free internet ecosystem (American users); and on the other side are users whose only choice of communication with those abroad is WeChat (Chinese users).

[151] See, eg, Louise Matsakis, 'TikTok is Paying Creators. Not All of Them are Happy' (*WIRED*, 10 September (Sept 10, 2020), <https://www.wired.com/story/tiktok-creators-fund-revenue-sharing-complaints/> accessed 19 April 2021. *Cf* Taylor Lorenz, 'What if the U.S. Bans TikTok' *The New York Times* (10 July 2020), <https://www.nytimes.com/2020/07/10/style/tiktok-ban-us-users-influencers-taylor-lorenz.html> accessed 19 April 2021 (noting that users are feeling "anxiety," including for users whom "TikTok is their livelihood.").

usage of an app. Indirectly, this might be content-neutral, which lowers scrutiny.[152] However, by targeting specific types of apps—for example, primarily Chinese-speaking (WeChat); primarily used by younger users (TikTok); or those that focus on a specific demographic or theme—the government might be intentionally or unintentionally curtailing content-specific speech. Again, the risks articulated above could be pretextual and could help frame a technology ban as a time/place/manner restriction, rather than one that aims at specific types of speech, lowering the type of scrutiny courts apply.

Ultimately, courts are yet to determine the factors considered in the First Amendment context when looking at app bans. But even the threat of such bans may come at the price of uncertainty and chilled speech, especially if users switch away from these platforms in the face of threats to ban communication tools.

B. Undermining Internet Freedom, Human Rights, and American Foreign Policy

American efforts to ban Chinese technologies play into the Chinese "cyber sovereignty norms" that support China's territorial vision of the internet, where each government plays a central role in shaping the governance of the internet within national boundaries. Instead of is opposed to allowing private actors to manage the flow of data and the ability of information.[153] Although China does not actively export "digital authoritarianism," other governments can gravitate towards these tools through emulation.[154] For the US—a government that has taken a hands-off approach to internet regulation—emulating China's approach of asserting a strong role for government officials to ban communications tools flies in the face of long-standing norms and protections. One of the main issues is that the US is not just blocking foreign technology agnostic to its origins; rather, it is specifically excluding *Chinese* technology as tensions between the two countries escalate.

In fact, given the nebulous, broad, and unclear risks defined in Section II, these technology bans may also have a more compelling, non-legal justification: great power politics intended to compete with growing Chinese cyber

---

[152] See, eg, *Reed v Town of Gilbert* 192 L Ed 2d 236 : 576 US 155, 166 (2015) (noting that content neutral laws are subject to a "lower level of scrutiny").

[153] Rogier Creemers, 'China's Conception of Cyber Sovereignty : Rhetoric and Realization' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (2020) 107.

[154] Matthew S Erie and Thomas Streinz, 'The Beijing Effect: China's' Digital Silk Road' as Transnational Data Governance' (2021) New York University J Intl L & Politics (JILP), Forthcoming.

power, resulting in a homegrown digital wall that emulates Chinese strategy. The US has concerns about national security regarding China's ability to gain intelligence benefits from controlling the exchange of global technology.[155] In the US, for instance, the government benefits from the dominance of American technology firms and the government's ability to demand data from firms for domestic and national security purposes.[156] The strategic vantage point that the US perceives China to be gaining is instilling fear that China will gain an upper hand to bargain with. This threat is heightened when foreign technology is used by US military or government officials, raising fears of blackmail and extortion.

Despite these concerns, US efforts to impose bans on communication technology may lead to more serious long-term consequences. These efforts play into Chinese "cyber sovereignty norms" that support China's vision of the internet, which promotes an alternative vision to the US Internet Freedom policy.[157] Since the dawn of the internet, dictators have viewed the internet as a potential threat to power. The Arab Spring served as a painful reminder for many leaders that communications tools could be used by organized opposition against the regime. China argues that governments should be able to control the internet, acceding to the demands of national security. But with these technology bans, the US has borrowed from China's toolkit in order to address security and sovereignty concerns by blocking access to a communications platform. Combined with other Western countries' shift to a more reasonable regulatory regime that penalizes technology companies (both foreign and domestic) for competitive and online harms,[158] the US's heavy-handed regulatory approach of banning technologies does much to normalize China's approach to internet governance.

These efforts have serious global consequences. First, American actions matter as cybersecurity norms continue to develop and the US and China compete to establish norms for internet governance.[159] China's vision is one that strongly supports state sovereignty and territorial control over

---

[155] Farrell & Newman (n 50).

[156] Alan Z. Rozenshtein, 'Surveillance Intermediaries' (2018) 70 Stanford L Rev 99. Of course, these demands are made through the courts and with sufficient legal protections for those subject to the surveillance.

[157] Creemers (n 153).

[158] See, eg, Australia's negotiations with Facebook about paying news outlets for hosting their links on the Facebook platform. Jason Scott and Vlad Savov, 'Australian Law Could Force Facebook, Google to Strip Content' (*Bloomberg*, June 22, 2021) <https://www.bloomberg.com/news/articles/2021-06-23/australia-s-online-safety-bill-forces-platforms-to-strip-content> accessed 16 August 2021.

[159] Laura De Nardis, *The Global War for Internet Governance* (Yale University Press 2014).

information flows.[160] The US government, on the other hand, supports a vision of a "borderless"[161] internet, where limited government interventions support and uphold global free speech protections. These differences are reflected in preferences for the application of existing human rights law as well as whether internet governance should be located in multistakeholder institutions (preferred by the US) versus multilateral institutions (preferred by China). Processes within the UN, supported by the US, aim to develop norms for cybersecurity and establish a common understanding.[162] US efforts to ban communications tools normalize the "cyber sovereignty" policy and could undermine US efforts at the UN to codify internet freedom norms into international agreements and processes.

Second, for a government that has promoted the free flow of information, US attempts to block communications tools create permissive space for other governments to implement similar bans. Goldsmith describes the failure of the internet freedom foreign policy as animating from the hypocrisy of US strategies.[163] One arm of the diplomatic core promotes free speech values and the right to access content, whereas more recent policies have undercut the message by blocking Chinese communication tools. Despite being a nation that strongly privileges free speech at home and abroad, these current American efforts diminish the reach of original foreign policies designed to limit digital walls and preserve a zone of openness and information exchange.

Because of the hypocritical policy that fuels justification for the Chinese approach to dealing with cybersecurity threats, other democratic governments may follow suit and adopt bans of their own to mirror US policy. This hypothesis is supported by theories of legal diffusion, which suggest that policy decisions are not made independently. As governments adopt particular legislation, their counterparts take note.[164] Emulation occurs when

---

[160] Cai Cuihong, 'China and Global Cyber Governance: Main Principles and Debates' [2018] 42 Asian Perspective 647; Creemers (n 157).

[161] 'Senior State Department Official on State Department 2019 Successes on Cybersecurity and 5G Issues' (*United States Department of State*, 9 January 2020) <https://2017-2021.state.gov/senior-state-department-official-on-state-department-2019-successes-on-cybersecurity-and-5g-issues/> accessed 25 April 2021.

[162] Martha Finnemore and Duncan B Hollis, 'Constructing Norms for Global Cybersecurity' [2016] 110 American J Intl L 425.

[163] Goldsmith & Wu (n 17).

[164] Beth A Simmons & Zachary Elkins, 'The Globalization of Liberalization: Policy Diffusion in the International Political Economy' [2004] 98 American Political Science Rev 171–189; Frank Dobbin, Beth A Simmons & Geoffrey Garrett, 'The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning?' [2007] 33 Annual Review of Sociology 449–472; Beth A Simmons, Frank Dobbin & Geoffrey Garrett, 'Introduction: The International Diffusion of Liberalism' [2006] 60 Intl Org, <http://www.journals.cambridge.org/abstract_S0020818306060267> accessed 19 April 2021; Zachary

governments adopt policies in a "follow the leader" approach, with policymakers considering laws from the largest or richest countries as standards that should be emulated.[165] An example of this is India's policy concerning Chinese apps. After a border clash with China, India retaliated by preventing an estimated 200 million users from accessing TikTok.[166] Other governments are also beginning to probe into the practices of TikTok: leaders from Japan's Liberal Democratic Ruling Party launched efforts to restrict access to TikTok and other Chinese-owned apps to protect personal information.[167]

The US vision has long been one of the dominant approaches to internet governance. As the architect of the internet, the US was able to instil preferences into many international institutions and forums.[168] Internet Freedom is also reflected in some multilateral decisions. Seeking to advance Article 19 protections of the Universal Declaration of Human Rights that guarantees that everyone enjoys the right to "to seek, receive and impart information and ideas through any media and regardless of frontiers," the UN Human Rights Council and General Assembly agreed that offline rights apply online.[169] Other victories include the Internet Freedom Coalition. In 2011, fourteen countries endorsed a declaration protecting human rights and fundamental freedoms online.[170] More recently, President Biden organized a partnership of "techno-democracies"[171] designed to prevent China from

Elkins, Andrew T Guzman & Beth A Simmons, 'Competing for Capital: The Diffusion of Bilateral Investment Treaties, 1960–2000' [2006] 60 Intl Org 811.

165 Dobbin, Simmons, and Garrett, ibid 452.

166 Raymond Zhong & Kai Schultz, 'With India's TikTok Ban, the World's Digital Walls Grow Higher' *The New York Times* (30 June 2020) <https://www.nytimes.com/2020/06/30/technology/india-china-tiktok.html> accessed 19 April 2021. We note that this happened around the same time that the Trump Administration banned TikTok, though who thought of the idea first is unclear. Even so, the US policy affirms and justifies the Indian policy.

167 Jennifer Hassan & Ruby Mellen, 'It's not just the United States: These Governments also see TikTok as a Problem.' *The Washington Post* (18 September 2020) <https://www.washingtonpost.com/world/2020/08/03/its-not-just-united-states-these-governments-see-tiktok-growing-problem/> accessed 19 April 2021.

168 Kal Raustiala, 'Governing the Internet' [2016] 110 American J Intl L 491 (specifically referring to US dominance over ICANN, the organization that handles the assignment of domain names).

169 n 3. See also David Kaye, 'The Limits of Supply-Side Internet Freedom' (*Knight First Amendment Institute,* 2018) <https://knightcolumbia.org/content/limits-supply-side-internet-freedom> accessed 29 March 2021.

170 'Launch of Internet Freedom Coalition at "Freedom Online" Conference' (*U.S. Department of State*, 13 December 2011) <//2009-2017.state.gov/r/pa/prs/ps/2011/12/178667.htm> accessed 29 March 2021.

171 Jared Cohen & Richard Fontaine, 'Uniting the Techno-Democracies' (*Foreign Affairs*) <https://www.foreignaffairs.com/articles/united-states/2020-10-13/uniting-techno-democracies> accessed 18 March 2021.

"setting the rules and shaping the norms that govern the use of technology."[172] However, these efforts are undermined by US domestic responses—including ones that are no longer in effect, like President Trump's technology bans[173]—that implicitly support a "cyber sovereignty" approach and deviate from long-standing efforts designed to instead design international collaboration to support free expression.

C. Data Storage and Localization

Another major issue within the Internet Freedom and cyber sovereignty debate is the concept of data localization. Data localization undermines the notion of an open internet through technical means, by requiring that companies store particular types of information within national borders.[174] The US government has sought to prevent the diffusion of data localization policies, even codifying clauses that prohibit data localization within major trade agreements.[175]

Continued scrutiny about foreign access to US user data, exacerbated by technology bans, may motivate companies to store user data in the US. A major concern driving these US government technology bans is the ability of hostile foreign governments like China to access US user data.[176] However, companies claim that their data is not stored in China, but elsewhere; in

---

[172] David Ignatius, 'Opinion | Biden's Ambitious Plan to Push Back against Techno-Autocracies' *The Washington Post* (11 February 2021) <https://www.washingtonpost.com/opinions/bidens-ambitious-plan-to-push-back-against-techno-autocracies/2021/02/11/2f2a358e-6cb6-11eb-9ead-673168d5b874_story.html> accessed 18 March 2021.

[173] Among the myriad reasons that even an obsolete and undone policy undermines the overall Internet Freedom message are the potential transitory nature of US foreign policy, which subsequent Presidents can easily change without significant Congressional approval; the signals sent to anti-democratic countries that create a permission structure for technology bans to take place; the uncertain investment atmosphere that may dissuade foreign companies from bringing their technology to the US; and the difficulty of undoing technology bans that have already gone into effect, like those in India.

[174] Anupam Chander & Uyên P Lê, 'Breaking the Web: Data Localization vs. the Global Internet' (2014) Emory L J, Forthcoming; Anupam Chander & Uyên P Lê, 'Data Nationalism' (2014) 64 Emory L J 677.

[175] Michael Giest, 'Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards' (*Centre for International Governance Innovation*, 2018) <https://www.cigionline.org/articles/data-rules-modern-trade-agreements-toward-reconciling-open-internet-privacy-and-security> accessed 23 April 2021; Agam Shah & Jared Council, 'USMCA Formalizes Free Flow of Data, Other Tech Issues' *The Wall Street Journal* (29 January 2020) <https://www.wsj.com/articles/cios-businesses-to-benefit-from-new-trade-deal-11580340128> accessed 23 April 2021.

[176] See s II.A.

TikTok's case, the company claims its data is stored on servers in the US and Singapore.[177]

But given the borderless nature of the internet, significant issues arise. First, it is unclear whether foreign nations or governments are prohibited from accessing data if that data is stored in the US. In TikTok's case, even though it claimed that its data was stored in the US and Singapore, the company noted that its information could still be shared with its China-based parent company, ByteDance, and other affiliates.[178] Second, logistical issues arise for users who travel: is data stored in the US based on whether the user is in the US, whether the server is in the US, or whether the user is a US person? Additionally, when a non-US person communicates with a US person, whose location controls where the data is stored?

Effectively, how the law defines "US person" may define how much data is stored in the US. If a "US person" includes not just citizens and those located in the US, but anyone using a US-based server, such a definition will be overinclusive, capturing more than just people physically located in the US. Further, a broad definition of a US person or storage of more than just US users' data in the US may lead to reciprocity by foreign states: other states may incentivize companies to store data pertaining to domestic users locally, and may do so in an over inclusive manner. This would harm the privacy of US users by allowing their data to be stored in other countries and be accessed by foreign governments without due process, and harm the privacy of foreign users by encouraging their home governments to store data locally, making it easy for them to access such data. Of course, this assumes that US users' data stored at home is more private than data stored abroad. In some cases—especially where "abroad" includes authoritarian countries or those with invasive governments, like China—this is evident. In other cases, this claim is subjective. However, having US users' data stored in the US provides more easily accessible courts where privacy concerns can be litigated and allow consumers to deal with a government that is at worst translucent,[179] but whose practices are familiar.[180]

---

[177] Robert McMillian, Liza Lin & Shan Li, 'TikTok User Data: What Does the App Collect and Why are U.S. Authorities Concerned?' *The Wall Street Journal* (7 July 2020) <https://www.wsj.com/articles/tiktok-user-data-what-does-the-app-collect-and-why-are-u-s-authorities-concerned-11594157084> accessed 19 April 2021.

[178] ibid.

[179] For example, the US's Freedom of Information Act requests provide Americans with the ability to access what kind of information the government collects about them. See 5 USC § 552.

[180] Another example of a familiar and somewhat transparent process is the stringent process required for the government to get a warrant to wiretap (including the monitoring of electronic communications) a suspect. The government must provide a variety of information,

The costs of such implications go beyond financial (including aggregation and efficiency losses) and logistical considerations. If data of non-US users is stored abroad, that may have a roundabout impact on national security, leaving data not stored on cloud servers, but on local servers, more difficult to reach by warrants like those considered in *United States v Microsoft Corp*.[181] Additionally, data localization may facilitate the ability of foreign governments to surveil their own citizens, by creating one local honeypot where data can be found, rather than creating jurisdictional hurdles. There may also be enhanced scrutiny of US data standards and surveillance practices if the definition of US users is overbroad and includes non-US persons, and could have reciprocity impacts. Finally, while some US trade agreements ban data localization (such as the US-Mexico-Canada Agreement), actions against companies that access US user data where data localization is not in place may effectively create de facto data localization by incentivizing companies to store their data locally for fear of punishment, without explicitly saying so legally.[182]

The issue of data localization is one that courts and policymakers have yet to completely comprehend. However, current technology embargoes and actions may bring about the need to tackle this issue head-on or risk creating the perverse incentives and side-effects of a de facto data localization law.

V. Conclusion

The saga of the TikTok ban and the Trump Administration are both in the past, even if temporarily. But while the administration was fleeting, the American strategy of banning foreign technologies, especially in light of the tense US-China relationship, may be unlikely to disappear. The threats that the US government presented to justify these bans—Chinese access to American consumer data, Chinese censorship, and Chinese election interference and disinformation campaigns—are vague and ill-defined. But the

including the identity of the officer making the application, detailed reasoning for why the wiretap is required, a limited period of time for when the wiretap can be implemented, and must ensure that the minimum amount of information is intercepted. See generally 18 USC § 2518. Of course, the government's mass national security surveillance programs after the Snowden program have shown the possibility that at least metadata is collected without due process. But generally speaking, where detailed information beyond metadata is collected, the process requirements indicate that some modicum of privacy may be preserved.

[181] 2018 SCC OnLine US SC 72 : 138 S Ct 1186 : 584 US ___ (2018).

[182] See, eg, Michael Geist, 'How the USMCA falls Short on Digital Trade, Data Protection, and Privacy' *The Washington Post* (3 October 2018) <https://www.washingtonpost.com/news/global-opinions/wp/2018/10/03/how-the-usmca-falls-short-on-digital-trade-data-protection-and-privacy/> accessed 19 April 2021.

threat of Chinese disruption to the US government's functionality is evident in light of the current cybersecurity and threat context. Despite this significant and well-articulated risk, the strategic costs of such bans, the impacts on speech and international relations, and the cost of precedent do not justify using the hammer of bans on foreign technology bans on problems that do not look like nails. And the lack of transparency in what these threats entail and how the decision-making process played out procedurally raise questions about the necessity and benefit of such bans.

We note that this article is a brief glimpse into the complex, arcane logic and the corresponding balancing act of foreign technology bans in the US. More work is required to create a holistic picture that incorporates not just the speech and international relations implications of such bans, but also the heavy costs to the data economy and the intelligence sector. Given the Indian government's ban on Chinese apps, future work could discuss the Indian government's even blunter approach to technology bans, which have been successfully implemented and have not been invalidated in courts. Notably, unlike the US, the Indian government does not have the shackles of an Internet Freedom policy to be beholden to. And the constraints and protections of the First Amendment do not apply in Indian law. These different circumstances, in combination with China's proximity and nearby military threat, may create a different set of costs and benefits. Additionally, the US's past technology bans could justify technology bans in other democracies, like in India.

Clearly, the Indian context is different, since the bans have been implemented. This raises a whole host of curious questions. Given these bans, what kinds of speech, if any, have been stifled? Have other countries, including China, retaliated by banning Indian technology? What kinds of justifications are considered legitimate in the Indian context, and do they mirror those used in the American context? These questions were beyond this paper's scope, but answering them might help create a more complete framework for categorizing threats, understanding their magnitude, assessing their validity, and highlighting how such bans are perceived by other countries that are also threatened by Chinese cybersecurity prowess.

Ultimately, however, from an American policy and legal perspective, the consequences of these bans are far-fetched and damaging. That the Biden Administration has not pursued them further provides us with some time to assess the harms, and pursue more targeted policies that do not affect speech, encourage censorship, and undermine Internet Freedom.