THE BANNING OF TIKTOK, AND THE BAN OF FOREIGN SOFTWARE FOR NATIONAL SECURITY PURPOSES

INTRODUCTION

On August 6, 2020 President Trump issued an executive order under the International Emergency Economic Powers Act (IEEPA) prohibiting all interactions between American citizens and the Chinese-based company ByteDance Ltd, essentially banning the use of the popular app TikTok in the United States.[1] Questions surrounding the legality of this ban emerged immediately.[2] While the Biden Administration reversed Trump's order, President Biden himself has implemented his own order regarding foreign developed technology, suggesting these cybersecurity issues will continue to persist.

The US is not the first country to attempt to prohibit its citizens from using an app created and owned by an out of state developer for security reasons. China and other countries have successfully enacted laws to keep certain foreign apps out of their citizens' hands.[3] To determine the

1 "[A]ction must be taken to address the threat posed by one mobile application in particular, TikTok." Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020), "TikTok automatically captures vast swaths of information from its users, including Internet and other network activity information such as location data and browsing and search histories. This data collection threatens to allow the Chinese Communist Party access to 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. TikTok also reportedly censors content that the Chinese Communist Party deems politically sensitive" *Id*.

2 "TikTok sued the U.S. government on Monday, accusing the Trump administration of depriving it of due process when President Trump used his emergency economic powers to issue an executive order that will block the app from operating in the country." Mike Isaac & Ana Swanson, *TikTok Sues U.S. Government Over Trump Ban*, N.Y. TIMES, https://www.nytimes.com/2020/08/24/technology/tiktok-sues-us-government-over-trump-ban.html (Aug. 26, 2020).

3 Paige Leskin, *Here Are All the Major US Tech Companies Blocked Behind China's 'Great Firewall'*, BUSINESS INSIDER (Oct. 10, 2019, 11:23 AM), https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5#soundcloud-17. Users can get around the ban by using a virtual private network ("VPN"). Lani Fried, *How to Get Around the Great Firewall of China*, TOO MANY ADAPTERS (Mar. 17, 2021), https://toomanyadapters.com/get-around-great-firewall-china/#:~:text=The%20easiest%20way%20to%20get,by%20%E2%80%9Cspoofing%E2%80%9D%20your%20location. "An app launched . . . in China [that] allows access to some content on Western social media sites long banned domestically such as YouTube, marking the first product by a major Chinese tech firm that helps internet users bypass the Great Firewall." Reuters Staff, *Chinese App Allows Small Glimpse Beyond 'Great Firewall'*, REUTERS (Oct. 10, 2020), https://www.reuters.com/article/us-china-tech-firewall/chinese-app-allows-small-glimpse-beyond-great-firewall-idUSKBN26V0GQ. Shortly after Tuber entered the app store it stopped functioning properly and then later disappeared from the app store less than a month after its launch. Barclay Ballard, *This App Helped Bypass China's Great Firewall, but Has Vanished Into Thin Air*, TECHRADAR (Oct. 15, 2020), https://www.techradar.com/news/this-app-helped-bypass-chinas-great-firewall-but-has-vanished-into-thin-air.

implications of executing these bans and whether they are justified, one must look at the various actions countries around the world have taken in response to perceived foreign technology threats and the costs incurred by those countries to enforce a ban on such perceived threats.

This note explores the possible consequences of President Trump's attempted TikTok ban by looking at what the effect has been when other countries have cited national security concerns to ban foreign-developed technology. First, the question of whether a US president has the power and legal justification to ban TikTok will be addressed. Many people have raised questions about the legality of the Trump administration's actions, including TikTok who took legal action against the government after the ban, claiming the administration lacked the justification to ban the app.[4] Next, this note will delve into what a ban might mean for the future of the United States by analyzing the impact of bans on foreign technology in China, India, and Germany. Finally, the possible implications of an outright ban of foreign technologies in the United States will be hypothesized based on studies of countries that have banned certain foreign technology. Draconian cybersecurity laws that keep out foreign technology can harm international cooperation, prevent the spread of ideas and information in violation of the right to expression[5], and allow countries to collect data from their citizens that amounts to a privacy violation.[6]

---

4 TikTok claims the ban by the Trump administration was taken without any opportunity for TikTok to be heard, therefore violating due process, and they claim the President exceeded his authority in issuing an order that violated the company's First Amendment right to free speech. TikTok also argues that Trump's national security justification are purely speculative. Bobby Allyn, *TikTok Sues Trump to Block U.S. Ban*, NPR (Aug. 24, 2020, 6:28 PM), https://www.npr.org/2020/08/24/901776584/tiktok-sues-trump-to-block-u-s-ban. *See also* Todd Spangler, *Trump's Unprecedented Bans of TikTok, WeChat Apps Slammed as Violating First Amendment*, VARIETY (Sept. 18, 2020, 12:03 PM), https://variety.com/2020/digital/news/trump-bans-tiktok-wechat-app-first-amendment-1234774871/.

5 By exercising full control over network providers in the country the Chinese government is able to control what its citizens do and do not have access to. Gerry Shih, *China's Draft Cybersecurity Law Could Up Censorship, Irk Business*, REUTERS (July 7, 2015, 10:11 PM), https://www.reuters.com/article/us-china-cybersecurity/chinas-draft-cybersecurity-law-could-up-censorship-irk-business-idUSKCN0PI09020150708. This is not just occurring in China; many other countries are adopting laws that have the power to censor what its citizens can see on the internet. Adrian Shahbaz & Allie Funk, *The Global Drive to Control Big Tech*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech (last visited Jan. 4, 2022).

6 Adrian Shahbaz et al., *User Privacy or Cyber Sovereignty?*, FREEDOM HOUSE, https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty (last visited Jan. 10, 2020). "Over the last decade, Chinese users' ability to exercise their human rights online has rapidly declined, making China the most repressive information environment in the world. An increasingly sophisticated surveillance and censorship machinery, citizens' arrest for online activities, and targeted network shutdowns have allowed the government to tighten its grip around an already restrictive online environment." *Id.* (footnote omitted).

I. CAN THE PRESIDENT LEGALLY BAN TIK TOK?

President Trump's attempt to cut off all interactions with TikTok developer ByteDance Ltd. was immediately met with backlash from TikTok and First Amendment rights advocates who questioned the legality of the ban.[7] The order "draws its legal authority from the International Emergency Economic Powers Act, which allows the president to regulate economic transactions in a national emergency. Past administrations have used it to punish foreign governments . . . but have never used it against a global technology company"[8] making the president's actions unprecedented behavior. The Trump administrations rationale for banning TikTok, which is shared by politicians who support the ban and stricter laws dealing with foreign tech entities generally, [9] is that because TikTok is a Chinese owned company, they can be forced by the government to share the data of its American users with China, thus posing a national security threat.[10] However, according to James Lewis, Senior Vice President and Director of the Center for Strategic and International Studies, the data collected by TikTok is not nearly as sensitive or important to national security as the data that was leaked by previous breaches in the past, such as the Equifax data breach of 2017,[11] and it is not as easy for the Chinese government to get the

7 Chris Cooke, *Donald Trump's TikTok Ban is Unconstitutional*, *Says TikTok*, COMPLETE MUSIC UPDATE (Aug. 25, 2020), https://completemusicupdate.com/article/donald-trumps-tiktok-ban-is-unconstitutional-says-tiktok/; Hina Shamsi et al., *Don't Ban TikTok and WeChat*, ACLU (Aug. 14, 2020), https://www.aclu.org/news/free-speech/dont-ban-tiktok-and-wechat/; Taylor Lorenz, *TikTok Ban? Creators and Fans Are Big Mad*, N.Y. TIMES (Aug. 2, 2020), https://www.nytimes.com/2020/08/02/style/tiktok-ban-threat-trump.html.

8 Isaac & Swanson, *supra* note 2. Under the IEEPA past presidents have prohibited transactions with those engaged in human rights abuses, narcotics trafficking, trade of rough diamonds, etc. CHRISTOPHER A. CASEY ET AL., CONG. RSCH. SERV., RL45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE (2020). The "IEEPA has become an important means to impose economic-based sanctions since its enactment; like TWEA, Presidents have frequently used IEEPA to restrict a variety of international transactions; and like TWEA, the subjects of the restrictions, the frequency of use, and the duration of emergencies have expanded over time. Initially, Presidents targeted foreign states or their governments. Over the years, however, presidential administrations have increasingly used IEEPA to target non-state individuals and groups, such as terrorists, persons who engage in malicious cyber-enabled activities, and certain persons associated with the International Criminal Court." *Id.*

9 "Policymakers' chief worry is that ByteDance could be forced to hand over TikTok's data on US users to the Chinese government, under the country's national security laws. TikTok has said it stores American user data on US-based servers that aren't subject to Chinese law; skeptics argue TikTok's parent, ByteDance, is ultimately a Chinese business that's still beholden to Beijing." Brian Fung, *TikTok is a National Security Threat, US Politicians Say. Here's What Experts Think*, CNN BUSINESS (July 9, 2020, 6:47 AM), https://www.cnn.com/2020/07/09/tech/tiktok-security-threat/index.html.

10 *Id.*

11 Megan Leonhardt, *Equifax to Pay $700 Million For Massive Data Breach. Here's What You Need to Know About Getting a Cut*, CNBC (July 22, 2019), https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html.

information as it may seem.[12] Also, while security vulnerabilities in TikTok's software were found that could allow hackers to gain control of TikTok accounts, TikTok engineers were receptive to the criticism and TikTok and made the necessary security adjustments.[13]

TikTok sued the Trump administration in response to the ban, claiming the administration "ignored due process" and "authorize[d] the prohibition of activities that have not been found to be 'an unusual and extraordinary threat'" to the nation's security.[14] Another legal concern raised in reaction to Trump's attempted ban is that it violates First Amendment rights.[15]

---

12 Fung, *supra* note 9. "'The Chinese government does not necessarily have unfettered real-time access to all companies' data . . . Chinese corporate actors are not synonymous with the Chinese government or the Chinese Communist Party, and have their own commercial interests to protect.'" *Id*. (quoting Samm Sacks).

13 *Id.*; Alon Boxiner et al., *Tik or Tok? Is TikTok Secure Enough?*, CHECK POINT RESEARCH (Jan. 8, 2020), https://research.checkpoint.com/2020/tik-or-tok-is-tiktok-secure-enough/. Another concern surrounding TikTok is its content and moderation policies. In China, TikTok took down content that was critical of the Chinese government. Already Trump has accused TikTok of being used to spread false information about the Covid-19 pandemic and other conspiracy theories. There is concern that the app can be used to spread misinformation or weaken US power and influence. *Id*. A good example of this discreditation of US power and influence, and in particular discrediting the president and his allies, is the TikTok account of Kelly Anne Conway's daughter, Claudia, who uses her platform to spread anti-Trump messages and spread information about the President. Rebecca Jennings, *Claudia Conway's TikToks, Explained*, VOX (Oct. 6, 2020, 4:10 PM), https://www.vox.com/the-goods/2020/10/6/21504707/claudia-conway-tiktok-covid-kellyanne-daughter. Also, a concern of censorship in the realm of social media that is becoming more prevalent is the ability for these companies to control what its users are allowed to share and what is blocked. During the election social media platforms started tagging all election related posts with a disclaimer saying the information posted by a user may not be true. This included tweets from the President and other candidates running for office. Karissa Bell, *How Social Media Platforms Are Handling the 2020 Election*, ENGADGET (Nov. 4, 2020), https://www.engadget.com/how-social-media-is-handling-2020-presidential-election-223643220.html. Twitter even went so far as to prevent Trump's tweets declaring premature victory from appearing on user's timelines and prohibited retweets and likes. *Id.* And most recently after an attack on the capital building Twitter has permanently suspended Donald Trump's twitter for "risk of further incitement of violence." Kate Conger & Mike Isaac, *Twitter Permanently Bans Trump, Capping Online Revolt,* N.Y. TIMES (Jan. 12, 2021), https://www.nytimes.com/2021/01/08/technology/twitter-trump-suspended.html. Twitter is an American company though so perhaps maybe the concern doesn't lie in a foreign company's ability to influence but rather the government's power to limit social media platforms, which can harm the government's influence. This is particularly important in today's political climate where people are quick to doubt authority and have very strong opinions about what the government should and shouldn't be doing. *60 Minutes*: *Is TikTok a Harmless App or a Threat to U.S. Security?* (CBS television broadcast Nov. 15, 2020).

14 *Why We Are Suing the Administration,* TIKTOK (Aug. 24, 2020), https://newsroom.tiktok.com/en-us/tiktok-files-lawsuit. TikTok argues, "[t]he Administration ignored the great lengths that TikTok has gone to in order to demonstrate our commitment to serving the US market[,]" and that the executive order not only denies due process but also "authorizes the prohibition of activities that have not been found to be "an unusual and extraordinary threat," as required by the International Emergency Economic Powers Act (IEEPA)[.]"

15 Tyler Sonnemaker & Paige Leskin, *Trump's Attempt to Ban TikTok and WeChat Could Face Legal Trouble For Infringing on Free Speech, According to a First Amendment Expert*, BUSINESS INSIDER (Aug. 6, 2020, 11:49 PM), https://www.businessinsider.com/trumps-tiktok-and-wechat-bans-could-violate-first-amendment-expert-2020-8.

TikTok's lawyers and First Amendment advocates have argued that a ban of the app would take away content creator's and user's freedom of expression.[16] Interestingly, TikTok has been used to critique governments across the world, including the Trump Administration.[17] Additionally, because software is considered speech, there is an argument that the ban discriminates based on the identity of the software developer, ByteDance.[18] It is unknown whether these arguments would hold up against the Trump administration's national security argument, although a district judge did find the ban to be improper under the IEEPA.[19] Also, with the Biden administration taking over, the TikTok ban has been replaced with a new order that calls for a broader review of foreign controlled applications.[20] This order is meant to "establish 'clear intelligible criteria' to evaluate national security risks posed by software applications connected to foreign governments." [21]

II. WHAT HAPPENED WHEN OTHER COUNTRIES ACTED AGAINST FOREIGN TECHNOLOGY?

With the rise of technology and globalization, many corporations began employing modern technology to expand their services to users in multiple

16 Anne D'Innocenzio & Matt O'Brien, *U.S. Judge Temporarily Blocks Trump's Move to Ban TikTok From App Store*, GLOBAL NEWS (Sept. 27, 2020, 10:47 PM), https://globalnews.ca/news/7362631/tiktok-ban-1st-amendment-rights/.

17 Nathaniel Sobel, *Trump's Ban on TikTok Violates First Amendment by Eliminating Unique Platform for Political Speech, Activism of Millions of Users, EFF Tells Court*, ELECTRONIC FRONTIER FOUNDATION (Sept. 14, 2020), https://www.eff.org/deeplinks/2020/09/trumps-ban-tiktok-violates-first-amendment-eliminating-unique-platform-political#:~:text=A%20ban%20on%20TikTok%20violates,considerations%20for%20the%20users'%20speech; Taylor Lorenz, *The Political Pundits of TikTok*, N.Y. TIMES (Apr. 29, 2020), https://www.nytimes.com/2020/02/27/style/tiktok-politics-bernie-trump.html

18 Sonnemaker & Leskin, s*upra* note 15 (quoting Kyle Langvardt; "Most First Amendment experts would consider the apps themselves to be "content," and therefore targeting TikTok and WeChat specifically is effectively discriminating against them in violation of the First Amendment freedom of speech. The companies express themselves by setting their own rules for what to take down and what to leave up, Content discrimination is unconstitutional unless the law is 'narrowly tailored' to serve a 'compelling governmental purpose . . . Most laws fail this test.").

19 A District Court judge found that "the IEEPA does not give the president authority to regulate or prohibit, either directly or indirectly, "the importation or exportation of 'information or informational materials" or "personal communication[s], which do[] not involve a transfer of anything of value." Todd Spangler, *Trump Administration Likely Exceeded Legal Authority with TikTok Ban, Judge Rules*, VARIETY (Sept. 28, 2020), https://variety.com/2020/digital/news/trump-tiktok-ban-exceeded-legal-authority-ruling-1234785547/.

20 Katie Rogers & Cecilia Kang, *Biden Revokes and Replaces Trump Order That Banned TikTok*, N.Y. TIMES (June 9, 2021), https://www.nytimes.com/2021/06/09/us/politics/biden-tiktok-ban-trump.html.

21 *Id.*

countries.[22] In response, most states have had to carve cybersecurity laws out of their national security laws to protect themselves against potential foreign technology threats.[23] Every decision a country makes regarding national cybersecurity has implications for that country. These decisions often have unintended and damaging results for human rights and international relations.

A. China

China is known for being notoriously strict regarding foreign software.[24] China's cybersecurity law, passed in 2016, gives the government expansive power in monitoring threats to the country's cybersecurity.[25] Article 1 of the Cybersecurity Law of the People's Republic of China, states that one of the law's purposes is to "safeguard cyberspace sovereignty."[26] By forcing electronic data to be stored locally—within China's borders—the nation-state can control what its citizens have access to and make it more difficult

22 Tripti Lamba & Harmeet Malhotra, *Role of Technology in Globalization with Reference to Business Continuity*, 1 GLOBAL J. ENTERPRISE INFORMATION SYSTEM 2 (2009), http://www.informaticsjournals.com/index.php/gjeis/article/view/2956#:~:text=Technology%20has%20enabled%20the%20software,a%20central%20actor%20in%20globalization.

23 79% of countries have cybercrime legislation, while 13% of countries lack cybercrime legislation. For a map of countries with and without cybersecurity legislation, see *Cybercrime Legislation Worldwide*, UNITED NATIONS CONF. ON TRADE AND DEV., https://unctad.org/page/cybercrime-legislation-worldwide (last visited Feb. 4, 2021). For Canada's cybersecurity laws, see *Cyberlaw Tracker: The Case of Canada*, UNITED NATIONS CONF. ON TRADE AND DEV., https://unctad.org/page/cyberlaw-tracker-country-detail?country=ca (last visited Jan. 9, 2021). For German data protection and privacy laws, see *Cyberlaw Tracker: The Case of Germany*, UNITED NATIONS CONF. ON TRADE AND DEV., https://unctad.org/page/cyberlaw-tracker-country-detail?country=de (last visited Jan. 9, 2021).

24 In 2016, China enacted a regulation that required game makers to get a license from the government in order to get their apps listed in popular app stores, such as the Apple app store and Google play store. Arjun Kharpal, *Apple Sets Deadline for Gaming Apps to Comply with Chinese Law as Government Tightens Grip,* CNBC (Feb. 28, 2020, 3:49 AM), https://www.cnbc.com/2020/02/27/apple-sets-deadline-for-gaming-apps-to-comply-with-chinese-law.html. According to Apple, this permission comes from the General Administration of Press and Publication of China. *Id.*

25 Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 60 (2018). In 2014, China created the Cybersecurity and Informatization Leading Group, led by president Xi JinPing. *Id.* at 64–65. For a translation of China's cybersecurity law, see Rogier Creemers et al., *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017),* NEW AMERICA (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

26 "This Law is formulated in order to: ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the informatization of the economy and society." *Id.*

for foreign countries to access Chinese data.[27] China's cybersecurity law also has strict regulations for network operators[28] and internet service providers[29] which include domestic and foreign social media platforms. The government exerts monitoring powers over these network providers and requires them to provide assistance to government security agencies.[30] For example, if "providers find any content prohibited by the Provisions or other laws and administrative regulations, they must immediately stop transmitting the information, delete the information, keep the relevant records, and report the matter to competent government authorities."[31] The government may also use security certification, inspection, and review to block foreign companies' access to China's market.[32] Noteworthy apps banned "from reaching the countries over 800 million internet users" include Facebook, Google, Snapchat, and Twitter.[33]

By creating cybersecurity laws that favor domestic technology, the Chinese government can prevent cybersecurity threats while fostering local innovation. China's cybersecurity law has been met with great criticism by foreign businesses, who are subject to greater state control by the broad scope of the law.[34] They argue the law emphasizes protectionism more than

---

27 Lee*, supra* note 25, at 68–69. This requirement prevents operators from using more efficient services that store data abroad, such as the cloud. *Id.* at 94. "Operators of 'critical information infrastructure' (CIIOs) are already required under the Cyber Security Law to store in China all personal data of Chinese citizens collected over a network. This data localisation provisions has been in force since the law came into effect in 2017." Richard Bird, *Where Are We Now with Data Protection Law in China?*, FRESHFIELDS BRUCKHAUS DERINGER, https://digital.freshfields.com/post/102fqnd/where-are-we-now-with-data-protection-law-in-china-updated-september-2019 (Sept. 11, 2019).

28 Laney Zhang, *Government Responses to Disinformation on Social Media Platforms: China*, *in* GOVERNMENT RESPONSES TO DISINFORMATION ON SOCIAL MEDIA PLATFORMS: ARGENTINA, AUSTRALIA, CANADA, CHINA, DENMARK, EGYPT, EUROPEAN UNION, FRANCE, GERMANY, INDIA, ISRAEL, MEXICO, RUSSIAN FEDERATION, SWEDEN, UNITED ARAB EMIRATES, UNITED KINGDOM 43 (2019), https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1180&context=scholcom. *See also* Lee*, supra* note 25, at 70–71. "Network operators must maintain a private information protection mechanism to keep user information strictly confidential." *China's Cybersecurity Law and its Impacts - Key Requirements Businesses Need to Understand to Ensure Compliance*, PROVITI, https://www.protiviti.com/CN-en/insights/china-cybersecurity-law-and-impacts#:~:text=Network%20operators%20must%20maintain%20a,keep%20user%20information%20strictly%20confidential.&text=Collection%20and%20usage%20of%20private,public%20and%20under%20users'%20consent (last visited Oct. 25, 2020).

29 Zhang, *supra* note 28; Creemers et al., *supra* note 25.

30 Creemers et al., *supra* note 25.

31 Zhang, *supra* note 28.

32 Carmen Chan, *Understanding China's Data Security Law: An Intro for Foreign Businesses*, MEDIUM (Jan. 10, 2019), https://medium.com/faun/understanding-chinas-data-security-law-an-intro-for-foreign-businesses-bedc7105231.

33 Leskin, *supra* note 3.

34 Emilio Iasiello, *China's Cyber Initiatives Counter International Pressure*, 10 J. STRATEGIC SEC.1, 8,11 (2017); Lauren Maranto, *Who Benefits from China's Cybersecurity Laws?*, CTR. FOR STRATEGIC & INT'L STUD. (June 25, 2020) https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws.

security.[35] Complying with these cybersecurity regulations is costly, especially for foreign private companies who wish to conduct business within the country.[36] Smaller companies cannot afford to comply with these strict laws so only big companies with ample resources are able to operate successfully in the country and as noted above, many of these bigger companies, Facebook and Google, for example, are banned.[37] This has opened up the door for Chinese domestic companies to operate in the country. China has many of its own social media applications operated by Chinese companies. For example, "Renren" is a replacement for Facebook and "Sina Weibo" is a substitute for Twitter.[38] While this gives domestic corporations a chance to flourish, preventing foreign technology from being used in the country can lead to less innovation and less opportunity for new technologies.

There are major concerns that China is using its restrictive cybersecurity law to infringe on citizens' privacy by controlling what their citizens have access to.[39] This could just be a difference between Western ideals and ideals of modern Chinese culture,[40] but it is likely more nuanced. Companies

---

35 *Id*.; Josh Chin & Eva Dou, *China's New Cybersecurity Law Rattles Foreign Tech Firms*, WALL ST. J. (Nov. 7, 2016, 3:38 AM), https://www.wsj.com/articles/china-approves-cybersecurity-law-1478491064.

36 Lee*, supra* note 25, at 95. *See also* Beibei Bao, *How Internet Censorship Is Curbing Innovation in China*, THE ATLANTIC (Apr. 22, 2013), https://www.theatlantic.com/china/archive/2013/04/how-internet-censorship-is-curbing-innovation-in-china/275188/ ("China's lack of innovation derives partially from entrepreneurs not knowing enough about the latest trends, something attributable to the closed nature of the country's Internet. Slow traffic -- even with tools to hop over the Great Firewall -- also hinders creativity."); Hanna Beech, *China's Great Firewall is Harming Innovation, Scholars Say*, TIME (June 2, 2016, 1:37 AM) https://time.com/4354665/china-great-firewall-innovation-online-censorship/.

37 *Id*.

38 "Sina Weibo" acts as a replacement for Twitter in China; "Renren" is a replacement for Facebook. Julie Meredith, *10 Chinese Social Media Sites You Should Be Following*, (Mar. 27, 2013), https://www.synthesio.com/blog/10-chinese-social-media-sites-you-should-be-following/.

39 Lee*, supra* note 25, at 90. "The government's attempt to purify online content through the Cybersecurity Law is evidenced by the CAC's recent imposition of huge fines on the country's three major Internet companies-Tencent, Baidu, and Sina. The three internet giants were held in violation of the Cybersecurity Law because they failed to properly manage their social media platforms as some users 'spread information of violence and terror, false rumors, pornography, and other information that jeopardizes national security, public safety, and social order.'" *Id.* at 92 (citing Charlotte Gao, *China Fines Its Top 3 Internet Giants for Violating Cybersecurity Law*, DIPLOMAT (Sept. 26, 2017), https://thediplomat.com/2017/09/china-fines-its-top-3-internet-giants-for-violating-cybersecurity-law/); *A Closer Look at China's Cybersecurity Law — Cybersecurity, or Something Else?*, ACCESS NOW (Dec. 13, 2017), https://www.accessnow.org/closer-look-chinas-cybersecurity-law-cybersecurity-something-else/.

40 "The Western idea of cybersecurity places more emphasis on technical threats and the Chinese idea places more emphasis on ideological threats." The Chinese government uses social media and other internet formats to promote social policy. Lee, *supra* note 25, at 90 (citing U.N. GAOR, 66th Sess., at 1, U.N. Doc. A/66/359 (Sept. 14, 2011)).

are required to report people to the government if they distribute illegal content, which allows the government to quickly arrest whoever distributed the illegal content and perpetuate the restricted spread of information in the country.[41] Not only do foreign and domestic developers with critical infrastructure have to store all of the data from their Chinese users within the country, but they also must pass a security review by the Chinese government.[42] The Chinese government exercises complete control over these service providers. Through their strict cybersecurity laws, China can restrict information their citizens have access to, by forcing service providers to take down information that does not align with the government's agenda.[43] For example, to do business in China, Apple must exercise strict control over what they allow Chinese citizens to download.[44] Apple has a system in place that rejects or removes apps that do not comply with China's laws. Since 2017, "roughly 55,000 active apps have disappeared from Apple's App Store in China, with most remaining available in other countries."[45] Apple also stores its Chinese customers data in China on computers owned by a Chinese state-owned company and

41 "These concerns become even deeper if you look at Article 24 and 37 in the context of other provisions in the CSL. For instance, Article 48 requires private companies to censor expression and report people to the government if they publish or disseminate "illegal" content. Real-name registration would allow the government to identify and quickly arrest the person who creates vaguely defined "illegal" posts. And with the real-name information, the government could also quickly associate this person with posts on other websites, especially with the help of Article 28, which requires network operators to provide technical support and assistance to government agencies for national security or crime investigation purposes. "National security" will be defined under the National Security Law (NSL), which encompasses a broad range of issues, including finance, energy, and food. These laws ensure that the Chinese government has extremely broad authority to take action in response to published content." *A Closer Look at China's Cybersecurity Law — Cybersecurity, or Something Else?*, ACCESS NOW, (Dec. 13, 2017) https://www.accessnow.org/closer-look-chinas-cybersecurity-law-cybersecurity-something-else/.

42 Nabil Alsabah, *China's Cyber Regulations: A Headache for Foreign Companies*, MERICS (Mar. 22, 2017), https://merics.org/en/short-analysis/chinas-cyber-regulations-headache-foreign-companies.

43 Amar Toor, *China's New Cybersecurity Law Draws Criticism from Tech Companies and Rights Groups*, THE VERGE (Nov. 7, 2016), https://www.theverge.com/2016/11/7/13548648/china-cybersecurity-law-hacking-terrorism-censorship.

44 "Apple complied with Beijing's demand that it remove a number of VPN apps from its Chinese App Store that allow local users to visit blocked sites. And more recently, it removed Microsoft Corp.'s (MSFT) - Get Report Skype, which had run afoul of a government crackdown on foreign communications apps. The moves follow the 2016 removal of the New York Times' app, and the 2015 removal of the Apple News app." Eric Jhosna, *Apple and Google Are Doing Business in China Very Differently, and the Stakes Are High*, THE STREET (Dec. 6, 2017), https://www.thestreet.com/opinion/apple-and-google-s-very-different-approaches-to-china-have-huge-financial-consequences-14229937. Apple is also opening a data center in China to comply with their strict regulations. Paul Mozur et al., *Apple Opening Data Center in China to Comply With Cybersecurity Law*, N.Y. TIMES (July 12, 2017), https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html.

45 Jack Nicas, *Apple's Compromises in China: 5 Takeaways*, N.Y. TIMES (June 14, 2021) https://www.nytimes.com/2021/05/17/technology/apple-china-privacy-censorship.html.

shares its customers data with the Chinese government.[46] Previously, you could access outlawed apps and news outlets by using a VPN, but the government has cracked down on that as well, only allowing citizens and visitors to have access to information the government permits.[47] One of the important areas that China regulates is expression of democratic ideals. Only senior members of the Chinese Communist Party can publish information critical of the government[48] and those who do try to use the Internet for this purpose will likely be arrested under China's cybersecurity law.

B. India

India's Information Technology Act of 2000 ("IT Act"),[49] amended in 2008,[50] provides the primary source of protection for electronic data in India. Unlike China, India currently does not have a specific cybersecurity law.[51] Instead, it has a framework for rules and regulations that has proven inadequate to fully protect its citizens' data,[52] especially data on the cloud and data analytics that track internet behavior patterns.[53] Technology has advanced faster than the law though, causing a prevalence of cyberattacks in India.[54] India recently cited national security purposes to ban over sixty Chinese phone apps, including the ban of Chinese-owned TikTok.[55] Section

46 *Id*.

47 Josh Summers, *Why You (Still) Need A VPN In China In 2021*, CHINA EXPAT SOCIETY (Jan. 2, 2021), https://www.chinaexpatsociety.com/technology/why-you-need-a-vpn-in-china.

48 *Freedom of Expression in China: A Privilege, Not a Right*, CONGRESSIONAL-EXECUTIVE COMMISSION ON CHINA, https://www.cecc.gov/freedom-of-expression-in-china-a-privilege-not-a-right (last visited Mar. 21, 2021).

49 *View the IT Act 2000*, GOVERNMENT OF INDIA, https://www.meity.gov.in/content/view-it-act-2000 (Sept. 8, 2015).

50 The Information Technology (Amendment) Act, 2008 (In.).

51 Saheli R. Choudhury, *India's Existing Data Privacy Laws Are Inadequate in Protecting People's Information,* CNBC (July 13, 2020, 9:39 PM), https://www.cnbc.com /2020/07/14/india-chinese-apps-ban-data-protection-laws.html.

52 *Id. See also Indian Laws Inadequate to Deal with Data Theft: Experts*, INDIA TIMES (Apr. 2, 2018, 8:57 AM), https://ciso.economictimes.indiatimes.com/news/indian-laws-inadequate-to-deal-with-data-theft-experts/63574664; Divij Joshi, *A Comparison of Legal and Regulatory Approaches to Cyber Security in India and the United Kingdom*, THE CENTRE FOR INTERNET AND SOCIETY, (NOV. 12, 2017), https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf.

53 Ishveena Singh, *India's Cybersecurity Laws Inadequate for IoT, Big Data, Cloud and AI*, GEOSPATIAL WORLD (Apr. 7, 2017), https://www.geospatialworld.net/blogs/iot-big-data-cloud-and-cybersecurity-laws-in-india/.

54 *Id.*

55 Maria Abi-Habib, *India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat,* N.Y. TIMES (June 30, 2020), https://www.nytimes.com/2020/06/29/world/asia/tik-tok-banned-india-china.html. Cybersecurity experts say Chinese apps pose security risks because of China's National

69(A) of the IT Act permits the government to block access to information that is "prejudicial to [the] sovereignty and integrity of India, defense of India, security of state and public order."[56]

India is currently proposing a new cybersecurity law that would further strengthen the control the government has over technology.[57] Like the law in China, the proposed act would allow the government to require data to be stored locally in India and calls for "processing of data in the interests of security of the state," which would give law enforcement easy access to data and permit law enforcement to use that data.[58] With control of this data comes the same human rights concerns that are present in China, people being arrested for merely posting information on the internet which conflicts with the government's ideals.[59] Additionally, there are privacy rights concerns associated with the law. The new law would allow the government to collect and process any data from India's residents from any internet

---

Intelligence Law, which requires Chinese companies to support Chinese intelligence gatherings, meaning China could potentially be collecting data from TikTok's users. *Id.* India's ban of Chinese apps occurred after a border dispute between China and India. India, one of TikTok's biggest consumers, was likely motivated by these border disputes to ban Chinese Apps. The ban could have a real impact on China's economy. *Id*. *See also* Zak Doffman, *TikTok May Lose Up To $6 Billion As Result of India Ban; Users Urged to Delete App*, FORBES (July 4, 2020, 4:14 AM), https://www.forbes.com/sites/zakdoffman/2020/07/04/tiktok-loses-6-billion-as-users-urged-delete-app-immediately/#2404fa481c98.

56 *View the IT Act 2000*, GOVERNMENT OF INDIA, https://www.meity.gov.in/content/view-it-act-2000 (Sept. 8, 2015). "The IT Act underwent changes as Internet technology grew. In 2008, additions expanded the definition of "communication device" to include mobile devices and placed owners of given IP addresses responsible for distributed and accessed content. Privacy was addressed in 2011 when stringent requirements for collecting personal information came into effect. The most controversial change in this act involves section 66A. It makes "offensive messages" illegal and holds the owners of servers responsible for the content. That means if an IP address with pornographic images is traced to your servers, you can be held liable for it even if you did not authorize its access. Penalties arrange from imprisonment of three years to life and fines. Offenses that occur in a corporate setting can result in further administrative penalties and bureaucratic monitoring that can prove burdensome to doing business." *India IT Act of 2000 (Information Technology Act)*, TERMSFEED (Dec. 21, 2020), https://www.termsfeed.com/blog/india-it-act-of-2000-information-technology-act/.

For how one can challenge the blocking of an app that is a threat to national security in India, see Vaibhav Parikh, *Technology Turmoil: The Impact of India Banning Chinese Apps*, LEGAL TECH NEWS (Aug. 12, 2020), https://www.law.com/legaltechnews/2020/08/12/technology-turmoil-the-impact-of-india-banning-chinese-apps/?slreturn=20200923140703.

57 Manish Singh, *India Proposes New Rules to Access its Citizens' Data*, TECH CRUNCH (Dec.10, 2019, 5:41 AM), https://techcrunch.com/2019/12/10/india-personal-data-protection-bill-2019/.

58 Chinmayi Arun, *Three Problems with India's Draft Data Protection Bill*, COUNCIL ON FOREIGN RELATIONS (Oct. 3, 2018), https://www.cfr.org/blog/three-problems-indias-draft-data-protection-bill.

59 "The new proposals require proactive filtering and cleaning of online content by online platforms . . . This has striking similarities to China's demands towards global platforms to comply with its regulatory requirements where the legality of speech to a large degree is determined by cultural sensitivity." Neha Thirani Bagri*, India Proposes Tough New Laws to Censor Online Content*, L.A. TIMES (Jan. 11, 2019), https://www.latimes.com/world/la-fg-india-internet-censorship-2019-story.html (quoting Apar Grupta).

platform and use that data in the interests of security of the state.[60] This would give the Indian government unprecedented access to information about its own citizens.[61]

C. Germany

The EU has its own system for dealing with cybersecurity – the General Data Protection Regulation ("GDPR"), which is considered one of the most protective data laws in the world.[62] The GDPR works by imposing hefty fines on any organization that collects the data of people in the EU in a way that violates the GDPR's privacy and security standards.[63] The GDPR requires companies to be transparent with data processing, showing that the data they collect is for legitimate purposes, and getting consent from users.[64] Several countries in the EU have begun investigations into TikTok,[65] yet the

60 Arun, *supra* note 58.

61 *Id*.

62 "The EDPB is an EU body in charge of the application of the General Data Protection Regulation (GDPR) as of 25 May 2018." *What is the European Data Protection Board (EDPB)?*, EUROPEAN COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en (last visited Oct. 23, 2020). "The EDPB will be at the centre of the new data protection landscape in the EU. It will help ensure that the data protection law is applied consistently across the EU and work to ensure effective cooperation amongst DPAs. The Board will not only issue guidelines on the interpretation of core concepts of the GDPR but also be called to rule by binding decisions on disputes . . ." *Id.*; *What is GDPR, the EU's New Data Protection Law?*, GDPR, https://gdpr.eu/what-is-gdpr/ (last visited Oct. 23, 2020).

63 *What is GDPR, the EU's New Data Protection Law?*, GDPR, https://gdpr.eu/what-is-gdpr/ (last visited Oct. 23, 2020). *See also* Matt Burgess, *What is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Mar. 24, 2020), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018. For a guide on what companies have to do to avoid fines and fulfill the requirement of the GDPR, see *Everything You Need to Know About GDPR Compliance*, GDPR, https://gdpr.eu/compliance/ (last visited Oct. 23 2020).

64 *What is GDPR, the EU's New Data Protection Law?*, *supra* note 62. The strict regulations imposed by the GDPR seems to disadvantage smaller companies who cannot afford to comply with the regulations. Ivana Kottasová, *These Companies Are Getting Killed by GDPR*, CNN (May 11, 2018, 6:39 AM), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html. *See also How the GDPR Impacts and Suffocates Small and Medium Businesses*, I-SCOOP, https://www.i-scoop.eu/gdpr/gdpr-small-medium-businesses/ (last visited Oct. 25, 2020).

65 "The French authority, CNIL, is looking at a number of issues, including how the company communicates with users and the protection of children, a spokesman said Tuesday. The questions are part of an investigation into TikTok's plan to set up a European Union headquarters for data purposes." Helene Fouquet, *TikTok Faces French Data Probe, Adding to EU-Wide Scrutiny*, BLOOMBERG (Aug. 11, 2020, 12:30 AM), https://www.bloomberg.com/news/articles/2020-08-11/tiktok-faces-probe-from-french-privacy-watchdog-after-complaint. "The Dutch privacy watchdog said on Friday it would investigate how Chinese-owned social media app TikTok, which has become hugely popular during the COVID-19 pandemic, handles the data of millions of young users." Reuters Staff, *Dutch Watchdog to Investigate TikTok's Use of Children's Data*, REUTERS (May 8, 2020, 8:45 AM), https://www.reuters.com/article/us-netherlands-dataprivacy-tiktok/dutch-watchdog-to-investigate-tiktoks-use-of-childrens-data-idUSKBN22K1UE.

EU has taken no official action against TikTok and most EU countries have suggested they are not concerned with it.[66]

Each country in the EU also has its own protections for national security. Germany's cybersecurity laws are found in the Federal Data Protection Act,[67] which was written to coincide with the GDPR.[68] The Federal Data Protection Act has stricter requirements than the GDPR, such as the requirement for companies to employ a data protection officer, additional limitations for processing data, and further restrictions on data from scientific research.[69] The government of Germany used the Federal Data Protection Act to ban an American-made toy, My Friend Cayla, that listened and talked to the user of the toy.[70] The Federal Network Agency stated the toy's ability to hide broadcast cameras or microphones allowed it to "pass on data unnoticed and endanger people's privacy" and that the toy was a hidden espionage device that posed a risk to the youngest consumers.[71]

Germany has yet to take a stance on the possible security threats posed by TikTok, but "[a] German government official said the country has seen no signs that the app poses a security risk and has no plans to ban it."[72] Like

66 Vincent Manancourt, *TikTok Finds Safe Haven in Europe*, POLITICO (Aug. 6, 2020, 6:00 AM), https://www.politico.eu/article/tiktok-europe-safe-haven-us-china-tech-standoff/.

67 *Federal Data Protection Act (BDSG)*, FEDERAL MINISTRY OF JUSTICE AND CONSUMER PROTECTION (June 30, 2017), https://www.gesetze-im-internet.de/englisch_bdsg/.

68 *Id.*

69 Axel Spies, *Germany Enacts GDPR Implementation Law*, MORGAN LEWIS (June 6, 2018), https://www.morganlewis.com/pubs/germany-enacts-gdpr-implementation-law.

70 David Emery, *'My Friend Cayla' Doll Records Children's Speech, Is Vulnerable to Hackers*, SNOPES (Feb. 24, 2020), https://www.snopes.com/news/2017/02/24/my-friend-cayla-doll-privacy-concerns/; *German Parents Told to Destroy Cayla Dolls Over Hacking Fears*, BBC (Feb. 17, 2017), https://www.bbc.com/news/world-europe-39002142; Soraya Sarhaddi Nelson, *Germany Bans 'My Friend Cayla' Doll Over Spying Concerns*, NPR (Feb. 20, 2017, 4:40 PM), https://www.npr.org/2017/02/20/516292295/germany-bans-my-friend-cayla-doll-over-spying-concerns.

71 *Federal Network Agency Pulls Child Doll "Cayla" Out of Circulation*, BUNDESSNETZAGENTUR (Feb. 17, 2017), https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html?nn=265778. "To ban the doll in Germany, regulators invoked a federal law against espionage devices. And because that law provides fines of up to 25,000 euros for anyone who insists on selling or owning the equipment." Bill Chappell, *Banned In Germany: Kids' Doll Is Labeled An Espionage Device*, NPR (Feb. 17, 2017 11:51 AM), https://www.npr.org/sections/thetwo-way/2017/02/17/515775874/banned-in-germany-kids-doll-is-labeled-an-espionage-device.

72 Thomas Seal, *Europe Resists TikTok Ban as U.S. Advances China Tech Crackdown*, BLOOMBERG (Aug. 3, 2020), https://www.bloomberg.com/news/articles/2020-08-03/europe-resists-tiktok-ban-as-u-s-advances-china-tech-crackdown#:~:text=A%20German%20government%20official%20said,President%20Trump%20about%20the%20issue. Germany will also not block Huawei's 5G Netwoks from being used in Germany but will impose regulation on them. President Trump wanted for all of his allies to ban the Chinese companies' networks from their countries. Andreas Rinke, *Merkel's Conservatives Stop Short of Huawei 5G Ban in Germany*, REUTERS (Feb. 11, 2020), https://www.reuters.com/article/us-germany-usa-huawei/merkels-conservatives-stop-short-of-huawei-5g-ban-in-germany-idUSKBN205146.

many countries, Germany's cybersecurity laws have strengthened over the years to protect against increasingly sophisticated cybersecurity attacks.[73] While strengthening cybersecurity laws for national security reasons is a legitimate and proper justification, there are serious implications for people living in countries with these heightened national security laws. First, as in China where the government has banned certain foreign developed apps that can bring information which the government does not support, strict cybersecurity laws can create a deficiency in information. Social media platforms, in particular, spread information globally. If a social media platform is not allowed to operate in a country because it does not comply with that country's cybersecurity laws, then the citizens of that country are barred from accessing potentially valuable information that is being spread through that platform. A decline in the spread of information inevitably results in a regression in the spread of ideas and innovation. This regression leads the world away from globalization and toward a more nationalistic approach where countries will use internet sources that are operated and controlled by the countries they were created in.[74]

III. POSSIBLE IMPLICATIONS FOR THE UNITED STATES BASED ON THE IMPACTS OF FOREIGN TECHNOLOGY BANS IN OTHER COUNTRIES.

While the world-wide trend seems to be toward increasing cybersecurity laws and imposing more limitations on foreign technology, these limitations are not without consequence. If the United States did ban TikTok, another global power will have affirmed the ability of its government to influence the cybertechnology field. By examining the implications of bans on foreign technology in other countries, one can extrapolate the likely impact of the ban in the United States.

---

73 Detlev Gabel, *Germany's Draft Bill on IT Security 2.0 – Extended BSI Authorities, Stricter Penalties and New Obligations on Providers*, JD SUPRA (July 15, 2019), https://www.jdsupra.com/legalnews/germany-s-draft-bill-on-it-security-2-0-55094/.

74 Steven Aftergood, *Cybersecurity: The Cold War Online*, 547 NATURE 30, 30–31 (2017). Proponents of "free internet" argue for the free spread of information and transparency, while those who want greater control of the internet and information cite security reasons and the increase of hacking. According to Klimburg — director of cyber policy at the Hague Centre for Strategic Studies in the Netherlands, proponents of cyber sovereignty have an advantage. "They are, Klimburg says, perpetually on the offensive, using information as a weapon to advance national interests. The free Internet side, by contrast, struggles to defend a status quo based on international transparency and cooperation…Heightened concerns about online security are leading to increased governmental policing of cyberspace. Russian hacking of political campaigns and manipulative 'influence operations' during the 2016 US presidential election made dramatically clear the possibilities of weaponizing information. Rising nationalism and political polarization in the West may exacerbate the situation." *Id*.

When ousting foreign app developers, a country can still make its own similar apps for domestic users. India has done this after banning many Chinese apps. For example, there is an Indian version of TikTok called Bolo Indya.[75] An advantage of banning foreign developed technologies is that homegrown apps get more use and security breaches are less of a concern because the data is likely secured within the country.[76] Traditionally, many US tech companies have outsourced their data to servers in foreign countries but today data centers for US data are frequently being built within the US.[77] The United States could potentially generate similar benefits from a ban of TikTok, by creating its own domestic version of TikTok and other popular apps. Instagram, owned by the American company Meta, already runs a software similar to TikTok where users can make and watch short videos, called Reels.[78]

---

75 Priyadarshini Patwa, *Indian Alternative to Chinese Apps Like TikTok, CamScanner, Shein, and More*, ENTREPRENEUR INDIA (July 31, 2020), https://www.entrepreneur.com/article/354095.

76 Indian users are moving to Indian apps in place of TikTok. India has replacements for other Chinese apps that have been banned as well such as Shein, Clash of Kings, and other gaming apps. *Id.*

77 Facebook has three operational data centers it has built and manages on its own in Europe, located in Sweden, Denmark, and Ireland, and one under construction in Singapore. Like in North America, the company also leases data centers in Europe and Asia. Yevgeniy Sverdlik, *Facebook Plans Huge Expansion of Already Massive Georgia Data Cente*r, DATA CENTER KNOWLEDGE (Sept. 17, 2020), https://www.datacenterknowledge.com/facebook/facebook-plans-huge-expansion-already-massive-georgia-data-center.

78 *Introducing Instagram Reels*, https://about.instagram.com/en-us/blog/announcements/introducing-instagram-reels-announcement (last visited Aug. 5, 2020). *See* Joe Hindy, *11 Best TikTok Alternatives and TikTok Apps for Android*, ANDROID AUTHORITY (Oct. 1, 2020), https://www.androidauthority.com/best-tiktok-alternatives-1140092/, for a list of other possible TikTok replacements in the United States. This raises issues of copyright; however, as long as TikTok's software code is not directly copied this is not likely a concern for now especially in America where copyright protections are generally weak. Paul Murty, *Facebook Launches Reels App to Compete with TikTok*, SMITH & HOPEN (Sept. 2, 2020), https://smithhopen.com/2020/08/12/facebook-launches-reels-app-to-compete-with-tiktok/. These laws may become more strict as technology advances, but for now it is quite easy to have similar technologies compete with one another without intellectual property violations, even when those technologies are based off one another. Ahmad Saleh et al., *IP Protection of Software Innovations*, LEXOLOGY (Mar. 1, 2020), https://www.lexology.com/library/detail.aspx?g=ea6088f3-6413-4d2f-b1e3-6771f9120303. "Patent protection should be distinguished from copyright protection which is the easy route to protect computer programmes and software. Copyright protection is generally available for software developers in most countries and secured under several international conventions as well as local laws. However, although copyright protects the 'literal expression' of computer programmes; to say the source code against misappropriation or reproductions by non authorised parties, copyright does not protect the innovative concepts, features and processes underlying the software which often rely upon the core innovative and commercial valuable aspects of the software. This part, the innovative concepts, features and processes underlying the software, should be considered for protection under the patent route, where possible, and available in order to secure an appropriate level of protection for software developers. Absent patent protection of software related innovations, the legal protection of software will remain weak and vulnerable to misappropriation by others . . . Although hardware and other physical, tangible tangible inventions are patentable subject matter when they meet the patentability conditions of novelty and

Preventing foreign developers from bringing their technology or software to market can lead to a loss of freedom of expression for a country's citizens. A ban on TikTok could lead to a new level of censorship in America that is not consistent with Western ideals.[79] Perhaps, this explains why the European Union and Germany have yet to act against TikTok.[80] There is also an argument though that these platforms may lead to more censorship or a spread of ideas that are not consistent with democracy. In fact, TikTok was caught deleting content in China that was critical of China's government practices[81] and other social media platforms like Twitter and Instagram in America have censored or removed information that they categorize as overly violent or unreliable.[82] As technology advances and the number of electronic devices that the world

inventiveness, this is not always the case for software related innovations which follow a more complex legal scheme which varies from one country to another." *Id.*

79 For an understanding of China's perspective on cybersecurity and how it is different than western ideals, see Lee, *supra* note 25.

80 "The U.K. and France have no plans to block the ByteDance Ltd. platform in their countries, spokespeople for the governments said. A German government official said the country has seen no signs that the app poses a security risk and has no plans to ban it. A spokesman for British Prime Minister Boris Johnson said that he hasn't spoken to President Trump about the issue." Thomas Seal, *Europe Resists TikTok Ban as U.S. Advances China Tech Crackdown*, BLOOMBERG (Aug. 3, 2020), https://www.bloomberg.com/news/articles/2020-08-03/europe-resists-tiktok-ban-as-u-s-advances-china-tech-crackdown#:~:text=A%20German%20government%20official%20said,President%20Trump%20about%20the%20issue.

81 "TikTok, the popular Chinese-owned social network, instructs its moderators to censor videos that mention Tiananmen Square, Tibetan independence, or the banned religious group Falun Gong, according to leaked documents detailing the site's moderation guidelines." Alex Hern, *Revealed: How TikTok Censors Videos That Do Not Please Beijing*, THE GUARDIAN (Sept. 25, 2019), https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing. *See also* Fanny Potkin, *Exclusive: ByteDance Censored Anti-China Content in Indonesia Until Mid-2020, Sources Say*, REUTERS (Aug. 13, 2020), https://www.reuters.com/article/us-usa-tiktok-indonesia-exclusive/exclusive-bytedance-censored-anti-china-content-in-indonesia-until-mid-2020-sources-say-idUSKCN2591ML ("Chinese tech giant ByteDance censored content it perceived as critical of the Chinese government on its news aggregator app in Indonesia from 2018 to mid-2020, six people with direct knowledge of the matter told Reuters.").

82 Kalev Leetaru, *Is Twitter Really Censoring Free Speech?*, FORBES (Jan. 12, 2018), https://www.forbes.com/sites/kalevleetaru/2018/01/12/is-twitter-really-censoring-free-speech/?sh=17f2ece565f5; Exec. Order 13,925, 85 FR 34079 (2020)

(Online platforms are engaging in selective censorship that is harming our national discourse. Tens of thousands of Americans have reported, among other troubling behaviors, online platforms "flagging" content as inappropriate, even though it does not violate any stated terms of service; making unannounced and unexplained changes to company policies that have the effect of disfavoring certain viewpoints; and deleting content and entire accounts with no warning, no rationale, and no recourse. Twitter now selectively decides to place a warning label on certain tweets in a manner that clearly reflects political bias.).

relies on grows, cybersecurity laws will become ever more important.[83] While national security is undeniably important, the abuse of the national security justification in the tech world could lead to censorship of ideas and the limiting of human rights.

Another concern with human rights and national security is that governments have been using cyber security laws to collect data on their own citizens, possibly violating rights to privacy.[84] While the data of US citizens is not as easily transferred to the government by private companies as it is in China and potentially India, the government can still request data from private corporations via court orders, and they in fact do so frequently under the guise of "national security reasons."[85] Companies tend not to notify consumers when their data is requested by the government because these requests usually come with gag orders, preventing the company from notifying its customer. [86] Companies involved, like Microsoft, are currently fighting in court to keep the government out of their data servers. [87]

Strengthening cybersecurity laws will likely force countries to make their own apps and technologies, leading to decreased interactions between countries and greater inequalities between less developed and more developed countries.[88] Scholars predict that China's economy will be

---

83 "According to the Organization for Economic Cooperation and Development's Digital Trade Service Restrictiveness Index, 13 of the 46 majority economies have increased their digital trade restrictions between 2014 and 2019, while only four countries reduced their restrictions." Keman Huang, *The TikTok Ban Should Worry Every Company*, HARVARD BUSINESS REVIEW (Aug. 28, 2020), https://hbr.org/2020/08/the-tiktok-ban-should-worry-every-company.

84 *Id.* "The new India data protection bill grants the government the ability to direct any company to provide it with anonymized and non-personal data upon request. If the government wants access to protected personal data, it merely has to invoke a concern about national security, the "sovereignty or integrity" of the state, relations with foreign countries or the incredibly vague "public order" to compel private companies to give it access. The law has changed from its original form announced to the public two years ago, at which time there was a provision requiring that the government follow lawful procedures to collect any sensitive data." Scott Ikeda, *New India Data Protection Bill May Give Government Unlimited Access to Citizen Data*, CPO MAGAZINE (Dec. 24, 2020), https://www.cpomagazine.com/data-protection/new-india-data-protection-bill-may-give-government-unlimited-access-to-citizen-data/.

85 Priya Anand, *How Often Does the Government Ask Companies for Your Data*?, MARKET WATCH (Apr. 23, 2016), https://www.marketwatch.com/story/how-often-does-the-government-ask-companies-for-your-data-2016-04-22.

86 *Id.*

87 Louise Matsakis, *Microsoft's Supreme Court Case Has Big Implications For Data*, WIRED (Feb. 27, 2018), https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/.

88 "China's lack of innovation derives partially from entrepreneurs not knowing enough about the latest trends, something attributable to the closed nature of the country's Internet. Slow traffic -- even with tools to hop over the Great Firewall -- also hinders creativity. For example, if people are unable to watch videos without frequent buffering on YouTube, they may get frustrated in the process of seeking inspiration." Beibei Bao, *How Internet Censorship Is Curbing Innovation in China*, THE ATLANTIC (Apr. 22, 2013), https://www.theatlantic.com/china/archive/2013/04/how-internet-censorship-is-

negatively impacted by the loss of India's TikTok business.[89] Likewise, a ban on TikTok in the US could negatively impact the US. If other countries follow the trend of banning foreign software in favor of domestic software, then each country may develop their own social media platforms that store and control its data within that country to replace popular American made platforms such as Facebook or Twitter.[90] Relations between China and the United States are at a low point right now, with both countries accusing the other of misusing national security as an excuse to hurt their commercial competitors.[91] Relations between China and India are already strained due to an ongoing territorial dispute at their borders and these issues are heightened and prolonged by India's ban of certain Chinese developed applications.[92] Global communications should not break down over the use

curbing-innovation-in-china/275188/. Chinese researchers used to use VPN's to access information but the process was slow making research slower and costlier. This in turn slows down Chinese innovation. *Id.* China does have its own internet though which allows users to quickly access domestic sites like Baidu, China's google. *Id*.

89 "The ban significantly narrows a top growth market for Chinese technology firms and may embolden other governments to shut them out." *Ban on Chinese Apps: How It May Impact TikTok, Other Companies*, TIMES OF INDIA, https://timesofindia.indiatimes.com/business/india-business/ban-on-chinese-apps-how-it-may-impact-tiktok-other-companies/articleshow/76707803.cms (June 30, 2020); Manish Singh, *What India's TikTok Ban Means for China*, TECH CRUNCH (July 8, 2020, 12:56 PM), https://techcrunch.com/2020/07/08/what-indias-tiktok-ban-means-for-china/.

90 *See* Robert D. Hormatsus, *US Risks Falling Behind China on Technology and Innovation, If We Don't Reset Our Priorities*, THE HILL (July 14, 2019, 9:00 AM), https://thehill.com/opinion/technology/452694-us-risks-falling-behind-china-on-technology-and-innovation-if-we-dont-reset-our-priorities, for suggestion that the United States is falling behind in being one of the worlds' economic leaders. The United States currently runs the social media game, in that they own the most popular social media apps worldwide, but this also shows how much the United States has to lose if other countries begin to develop their own versions of these popular apps owned by the United States. Also, note that China also owns many popular apps on the list, most likely because their citizens do not have access to the same American apps like Facebook. For a list of the current most popular social networks worldwide, see J. Clement, *Most Popular Social Networks Worldwide as of July 2020, Ranked by Number of Active Users*, STATISTA (Aug. 21, 2020), https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. *See also* Charlie Campbell, *Inside the Controversial Company Helping China Control the Future of the Internet*, TIME (May 23, 2019, 6:38 AM), https://time.com/5594366/5g-internet-race-huawei/ ("This tech cold war matters because it could slow down or dramatically alter the rollout of a technology that is likely to define the future of the Internet for the next decade–the 5G networks in which Huawei has all but cornered the market . . . And right now, it looks like the U.S. is losing."); *Id.*

91 Joe McDonald, *China Criticizes US Order Against Dealing with Chinese Apps*, ASSOCIATED PRESS (Jan. 6, 2021), https://apnews.com/article/donald-trump-beijing-china-national-security-united-states-d76d5b39d7ee22006868f2efd1386aed.

92 Arshad R. Zargar, *India Bans TikTok and Dozens of Other Chinese Apps Amid Border Standoff*, CBS NEWS (June 30, 2020, 8:50 AM), https://www.cbsnews.com/news/india-bans-tiktok-other-china-made-apps-as-border-dispute-drags-on-today-2020-06-30/.

of an app, especially when there is not concrete proof that the app is a real national security concern.[93]

This is particularly important considering TikTok's willingness to cooperate with foreign countries and their cybersecurity laws. TikTok stated that it would be willing to store all its data locally and even has plans to create a data storage center in Ireland for its European users.[94] Furthermore, it is unknown whether TikTok is even sending the data it collects from its users to the Chinese government; for its part, TikTok denies these allegations.[95]

CONCLUSION

Cybersecurity laws should not further divide and create competition between countries, especially when that division could decrease innovation. Technology is developing and evolving at a rapid pace. The internet has brought about the opportunity for people living oceans apart to connect, enabling the sharing of ideas and information to create a world that is robust with knowledge and opportunity. This is especially true in the times of the COVID-19 pandemic. When England discovered a new, more contagious strand of COVID-19, that information was spread throughout the world and the strand was discovered in Colorado not long after the news was released.[96] Dissemination of that news through various apps provided people with more awareness and time to take precautions. While there is no data available yet, it will be interesting to analyze how the availability of

93 Zak Doffman, *Is TikTok Seriously Dangerous—Do You Need To Delete It?*, FORBES (July 11, 2020, 5:07 AM), https://www.forbes.com/sites/zakdoffman/2020/07/11/tiktok-seriously-dangerous-warning-delete-app-trump-ban/?sh=f03746c2b0e1.

94 Leo Kelion, *TikTok to Open $500m Data Centre in Ireland*, BBC (Aug. 5, 2020), https://www.bbc.com/news/technology-53664997#:~:text=TikTok%20has%20said%20it%20plans,up%20copy%20held%20in%20Singapore. For TikTok trying to create data storage center in India, see also Pankaj Doval, *TikTok to Government: Ready to Store Data Locally*, TIMES OF INDIA (July 29, 2020), https://timesofindia.indiatimes.com/business/india-business/tiktok-to-government-ready-to-store-data-locally/articleshow/77232329.cms#:~:text=NEW%20DELHI%3A%20TikTok%2C%20the%20blocked,emphasising%20that%20its%20operations%20always. "Though these practices have not yet helped TikTok to void the ban, they will probably be major arguments in its lawsuit against the U.S. Furthermore, these practices may be important directions that all companies might need to follow for doing international business in the new normal to address concerns over cybersecurity risks." Keman Huang, *The TikTok Ban Should Worry Every Company*, HARVARD BUSINESS REVIEW (Aug. 28, 2020), https://hbr.org/2020/08/the-tiktok-ban-should-worry-every-company.

95 Isaac & Swanson, *supra* note 2.

96 Amanda Macias, *Colorado Health Officials Are Investigating a Second Suspected Case of New Covid Strain*, CNBC (Dec. 30, 2020, 3:32 PM), https://www.cnbc.com/2020/12/30/new-covid-strain-colorado-health-officials-say-are-investigating-a-second-suspected-case.html.

the internet and even the presence of social media platforms impacted the effect of this virus in comparison to the 1918 influenza pandemic.

While many around the world can and do spend endless hours scrolling through the millions of short videos the TikTok platform offers, the app's future is still uncertain. With cybersecurity protections on the rise around the world and an unprecedented attempt by President Trump to ban TikTok, it is unclear whether in the future the US will be willing to accept apps like TikTok that have been developed by foreign countries.

If TikTok is banned in America, there is a good chance that other Western nations will follow suit.[97] By looking at the implications of foreign technology bans in China, India, and Germany, one can see what a ban could mean for the United States and other countries in the world. A national security concern does exist in the data collected and exchanged through foreign software. It is difficult to determine whether this national security threat is a valid reason to limit people's expression and access to information, and even more so when the national security concerns may just be a façade, hiding true political preferences or goals of censorship. In this case, the alleged national security threat does not significantly outweigh the benefits derived from apps like TikTok that promote freedom of expression and ideas and spread those ideas globally.

Although countries should protect against cyberthreats posed by other countries and there are valid national security reasons for increased cybersecurity laws, we must also be wary and cognizant that alternative motives, including government influence and/or suppressing competition, might be at play. We should not allow technology that promotes freedom of thought and the spread of ideas to be suppressed, especially when there is no proof of a national security concern that could justify the ban of a foreign technology.

Madison Clausius[98]

97 "[I]f there is a growing movement along the lines of what India has done and what the U.S. is considering, then we ought to consider it as well." Shruti Shekar, *Canada Needs Evidence of Data Misuse Before Considering TikTok Ban*, YAHOO FINANCE CANADA (July 14, 2020), https://www.yahoo.com/news/canada-would-ban-tik-tok-if-evidence-of-misuse-was-found-174321428.html (quoting Nathaniel Erskine-Smith).

98 Madison Clausius is an Executive Notes Editor at the Washington University Global Studies Law Review and a J.D. Candidate at the Washington University School of Law (2022).