WIIT SCHOLARSHIP ESSAY COVER PAGE

The attached essay is an abbreviated version of a much longer comment that I wrote as a staff editor of the *Temple International & Comparative Law Journal* (TICLJ) during the Fall 2020 and Spring 2021 semesters. While I received feedback from the professor who served as my faculty advisor, the writing is entirely my own. Please note that several sections were omitted and shortened, however, the full paper may be provided upon request.

THE *ULTRA VIRES* EFFECT: CFIUS'S OVERREACH OVER TIKTOK & THE NEED FOR U.S. FEDERAL DATA PRIVACY REGULATIONS

I. INTRODUCTION

Welcome to the Age of Big Data.[1] We live in a world where all our movements, choices, preferences, relationships, and interactions are collected as data points.[2] Every day, we give out personal data for free. However, personal data now has commercial value—data is being bought and sold in mass.[3] On an ordinary day, many people wake up to an alarm set by Amazon Alexa, which collects and stores recordings of all requests made.[4] Perhaps then you roll over and check the AccuWeather app for the weather to plan your outfit for the day, which collects data on your location.[5] If you commute to work, you might use the popular GPS navigation app Waze, which also collects location data.[6] Suppose you stop for a coffee at Starbucks and use the Starbucks app, which collects location, purchasing information, account information, and device and usage information, among other things.[7] The data is not just being gathered for the apps themselves—both AccuWeather and Waze have sold user location data to third parties.[8] All of these data touchpoints occur before you even step into the office and open your laptop.

To complicate matters further, your personal data can—and does—end up in the hands of those that may use that data for purposes that run contrary to "American ideals."[9] This is the basis for the TikTok saga: the "thorniest privacy dispute of 2020," which "actually isn't about privacy or technology at all—it's about China."[10] TikTok[11] is a Chinese-created mobile app that has exploded in popularity.[12] TikTok even landed the number two spot on Apple's most downloaded free apps list for 2020.[13] However, TikTok's increasing popularity has come with governmental scrutiny regarding the data that the app collects from its users.[14] In November 2020, an executive order issued by President Trump announced that TikTok would be banned—due to national

security concerns that Americans' personal data could be accessed by the Chinese government—unless ByteDance (TikTok's Chinese parent company) divests itself of that company.[15]

One theory of why the ban was issued was a personal vendetta of President Trump.[16] Regardless of the motivation behind it, the situation has brought significant attention to the activities of the Committee on Foreign Investment in the United States (CFIUS).[17] CFIUS rarely speaks about what the committee investigates due to confidentiality requirements prescribed by law,[18] therefore, it is incredibly unusual that there has been so much public discussion by the President, Secretary of State, and Treasury Secretary on the matter and that the case even went to the President at all.[19] CFIUS has the authority to review transactions where a foreign company is going to acquire or has acquired a U.S.-owned company. However, the U.S. government was incorrect in its assumption that this applies to TikTok, as it involves an intra-China transaction.

How can we remedy government overreach like the TikTok/CFIUS case in the future? This paper offers one possible idea: a general federal data privacy law to do so. The current state of data privacy legislation in the United States is not comprehensive enough to tackle data privacy issues of global mobile app companies. Consequently, the United States should look to enact comprehensive, federal data privacy legislation. The strongest data privacy law the world has seen to date, the General Data Protection Regulation (GDPR), was recently enacted in 2018 in the European Union and could serve as a framework for drafting and implementing such a law.

This paper is outlined as follows: Part II discusses the TikTok case in greater detail. Part III provides an overview of TikTok's data privacy concerns. Part IV describes how the E.U.'s GDPR can serve as a model for the creation of a much-needed federal data privacy regulation, noting that the United States can take lessons learned from unintended consequences of the GDPR and build an even better federal legislation of its own.

II. TIKTOK: FIERCELY POPULAR WITH USERS, BUT NOT WITH THE U.S. GOVERNMENT

TikTok is a social media app that has exploded in popularity over the last couple of years—it has been downloaded around two billion times and has nearly 700 million active users, of which 100 million are active U.S. users.[20] Contrary to its increasing popularity and user base, the U.S. government expressed national security concerns about the app.[21] President Trump issued two executive orders on the matter: the first banned any transactions with TikTok beginning forty-five days after the issuance of the executive order and the second requires that ByteDance divest its interest and rights in TikTok, as well as any data collected from its U.S. users.[22] In summary, U.S. national security concerns outlined in the Executive Orders stem from TikTok's collection of user data, the potential for it to track and blackmail federal employees, and its censorship of content.[23] Regarding the federal employee concerns, there is already a resolution in progress, the "No TikTok on Government Devices Act."[24] Recently passed in the Senate, if the House and President approve, it would prohibit employees with government-issued devices from downloading TikTok.[25]

Focusing on the second executive order, the authority to require that TikTok parent company ByteDance divest TikTok comes through congressional power delegated to the executive, exercised by CFIUS.[26] If CFIUS reviews a transaction and determines it to be a threat to national security, that threat cannot be otherwise mitigated by other U.S. laws, and there is "credible evidence" that allowing the transaction to proceed would impair national security, then CFIUS can block or suspend the transaction.[27] CFIUS can at any point review the transaction and force the parties to unwind the transaction or to comply with other required actions, such as a National Security Agreement, indefinitely.[28] This is the situation that TikTok is dealing with, as the acquisition of Musical.ly, which later became TikTok, by ByteDance occurred in 2017.[29]

However, there is one major element of this transaction that differs from the usual types of transactions that CFIUS reviews—both Musical.ly and ByteDance are Chinese-owned companies.[30] Take the case of Grindr, a gay dating app acquired by Chinese-owned Kunlun Tech in 2018. The Grindr acquisition raised national security concerns highly similar to those posed by TikTok, given analogous concerns over data privacy. As a result, CFIUS issued a decision requiring Kunlun Tech to fully divest from Grindr shortly after it acquired the company.[31] Despite those similarities, however, from a CFIUS perspective, there is an important difference between the TikTok and Grindr transactions, namely that Grindr was developed in Los Angeles before it was acquired,[32] and therefore involved the acquisition of a U.S. company by a Chinese company.

The transaction under investigation is the sale of Musical.ly, an app that was headquartered and created in Shanghai, China, managed in China, and owned by a majority of Chinese shareholders, to ByteDance, another company founded and developed entirely in China.[33] Musical.ly had a small U.S. presence, with 20 out of its 300 total employees based in the United States, who were not responsible for core operations, software or product development.[34] ByteDance also chose not to use Musical.ly's platform or source code in what makes today's TikTok technology platform—the platform used by TikTok was not acquired from Musical.ly but rather was developed by ByteDance before the acquisition.[35] The U.S. assets from Musical.ly that were integrated by ByteDance into TikTok were the Musical.ly app's user base and some licensing and copyright agreements.[36] The Divestment Order exceeded statutory authority because required divestment of the TikTok U.S. business in its entirety, while the "covered transaction" was only the U.S. business portion of Musical.ly as a whole that ByteDance acquired.[37]

In addition, while CFIUS has the jurisdiction to review transactions where a foreign company acquired a U.S.-owned company or U.S. assets, it cannot impose requirements on

companies solely because they sell services in the United States.[38] The concerns cited by the Executive Orders regarding TikTok were primarily focused on the national security threat posed by concerns about the way in which TikTok handles data privacy and the potential for the Chinese government to access that collected data.[39] The U.S. government's approach to resolving concerns about data privacy requires ByteDance to divest TikTok's U.S. assets, essentially forcing a Chinese company to sell a recent intra-China acquisition specifically to a U.S. company.[40] Not only is that an over-extension of CFIUS's authority because the "covered transaction" only relates to the specific U.S. assets acquired by ByteDance from Musical.ly and does not include the technology used in today's TikTok,[41] but there is another bizarre element of the demanded divestiture plan. President Trump wanted the United States to profit—he stated that the U.S. Treasury should get a "substantial portion" of the purchase price because it was making the transaction "possible" and that "[r]ight now they don't have any rights unless we give it to them."[42]

Furthermore, TikTok is currently suing the Trump Administration, as the company argues that it has already taken efforts to resolve these concerns and stores its U.S. user data with software barriers separate from other ByteDance products and from the reach of the Chinese government.[43] ByteDance also submitted several mitigation proposals prior to the divestment order in an attempt to address the national security issues and avoid judicial intervention.[44] However, all of ByteDance's mitigation proposals were rejected without CFIUS communicating a substantive response as to why the proposals were rejected.[45] Most recently, with the change to the Biden Administration, the Department of Commerce plans to conduct an evaluation of the justifications for the prohibitions against TikTok and whether those prohibitions are warranted. Until the new agency officials have had sufficient time to consider the issues in the case, which may eliminate the need for judicial review, the appeals will be held in abeyance.[46]

III. Overview of TikTok Data Privacy Concerns

Proposed solutions through the Executive Orders do not include changes to TikTok's data collection practices. Nonetheless, in the wake of the Executive Orders, there was heavy discussion in the public regarding whether Americans needed to delete the TikTok app from their phones for data privacy concerns.[47] In addition, several companies banned use of the TikTok app by employees.[48] Thus, an exploration of TikTok's data privacy practices, and whether these concerns are warranted compared to similar social media apps, is useful to understand what alternative options could resolve the national security concerns identified.

According to TikTok's privacy policy, the app automatically collects certain information from an individual when they are using the app, including IP address; geolocation data either based on information from the SIM card or IP address but not GPS data unless permission is given to do so; any messages sent through the app; device information such as device model, carrier, names other types of apps on the device, and what time zone the device is set in; metadata if content is uploaded to the app, e.g. captions, descriptions, or hashtags that accompany a video; and cookies.[49] Cookies are used to provide targeted advertising both on TikTok and outside the app—a practice not uncommon with mobile apps.[50] In comparing TikTok's privacy policy with other popular social media apps, the information collected and use of the information is substantially similar. In some cases, the other U.S.-based social media apps actually collect more information than TikTok, such as information about device signals like cell tower information.[51]

If TikTok's privacy practices aren't substantially different than those of other social media apps, then what's the problem? Again, "the key difference between U.S.-owned apps reviewed in the comparison above and TikTok is that there really isn't much of a firewall between Chinese tech companies and the Chinese state."[52] The major concern is that TikTok may hand over the

personal data of U.S. citizens to the Chinese government, a request TikTok claims it would deny if it were made.[53] While TikTok user data is currently stored in the United States and Singapore,[54] with data storage in the European Union in the works,[55] it is unclear whether TikTok could actually decline such a request, given that it is a Chinese entity.[56] TikTok's privacy policy states: "[w]e may disclose your information to respond to subpoenas, court orders, legal process, law enforcement requests, legal claims, or government inquiries."[57] On the other hand, TikTok took action to be removed from app stores in Hong Kong after a new Hong Kong-specific sedition law was passed that would require TikTok to provide data to China.[58]

Separately, given that one of the major concerns of the Trump administration was that a foreign government may be able to access the data, it is worth exploring security concerns surrounding Oracle, one of the U.S. companies that was planning to purchase a stake in TikTok.[59] President Trump approved a deal where Oracle and Walmart would be getting a combined 53% stake in TikTok Global, while the remaining ownership stake would go to ByteDance's Chinese and international investors.[60] Oracle would be responsible for reviewing both TikTok's source code and storing the data of American users.[61]

However, Oracle taking responsibility for the data security of TikTok might not be the saving grace the United States is seeking.[62] Commercial personal data gets stolen frequently, an issue from which Oracle has not been immune.[63] There was a major security breach at Oracle perpetrated by a Russian cybercrime group that resulted in personal data being made available to anyone on the internet.[64] Oracle taking over security for TikTok may end up with the same result—the potential for the personal information of users being made available to the parties that the United States seeks to prevent from acquiring that data through this transaction.[65]

VI. A PRACTICAL APPROACH TO DATA PRIVACY ISSUES WITH FOREIGN-OWNED COMPANIES: ENACTMENT OF FEDERAL COMPREHENSIVE DATA PRIVACY REGULATIONS LIKE THE GDPR

Given the absence of a comprehensive, federal data privacy law in the United States, the United States has relied on national security laws in order to regulate Chinese social media companies that obtain the data of U.S. users.[66] Using this approach, the President and CFIUS exceeded their authority, therefore, another avenue must be explored to provide another form of protection to American citizens to mitigate these national security concerns. This national security approach has been described as a "nationalist whack-a-mole, backed up with knee-jerk threats of expropriation,"[67] which undermines foreign investor confidence in the United States.[68] It is clear that the current state of data privacy legislation in the United States is not comprehensive enough to tackle data privacy issues of global mobile app companies—consequently, the United States should look to enact a federal, comprehensive data privacy legislation similar to the GDPR.[69]

A. The GDPR: The World's Strongest Data Protection Law

On May 25, 2018, the European Union passed the most comprehensive privacy and security law that the world has seen to date.[70] Penalties for non-compliance with the GDPR can reach the higher of 20 million euros or 4% of the preceding year's revenue for any company that violates its terms.[71] Since the inception of the GDPR, the Information Commissioner's Office (ICO) has issued notices of intention to fine Marriott over ninety-nine million euros and British Airways more than 183 million euros for breaches of the regulations.[72] Not only are the fines for non-compliance with the GDPR steep, but data subjects[73] themselves—the E.U. citizens who visit websites—can seek damages from the controller or processor that handles their data for GDPR infringement.[74] A controller or processor is an entity that handles personal data either within the organization that controls the website or through their provision of third party services to that organization. Moreover, the GDPR does not only apply to E.U.-based companies.[75] The regulation

reaches all activities involving the processing of personal data of E.U. citizens, regardless of whether the actual processing takes place in the European Union.[76] In order to not violate the GDPR rules surrounding transfers of personal data, companies are looking to establish data centers in the European Union.[77] For example, TikTok announced that it will be spending nearly $500 million to open a data center in Ireland.[78]

B. GDPR as a Data Protection Model – Is Everyone Convinced?

While the GDPR is a strong comprehensive data privacy regulation that can be used as a model for other countries like the United States, there are some unintended consequences from its enactment and some lessons learned that could be integrated.[79] The first unintended consequence is that the GDPR has been used to censor journalists who have published articles with personal data such as videos, photos and documents.[80] In Romania, journalists from the Rise reported on an alleged scam involving the President of Romania's Social Democratic Party, publishing screenshots of emails, photos, videos, and other forms of media that now involves regulated private data of Romanian citizens.[81] The Romania's Data Protection Authority ruled that the journalists violated Romania's data privacy law, which is based on the GDPR.[82]

Unfortunately, this was not an isolated occurrence. The same type of situation occurred in Slovakia, where head of Slovakia's data protection authority, Soňa Pőtheová, attempted to force an investigative outlet, Investigace.cz, to reveal anonymous sources by suggesting a 10 million euro fine.[83] Although Pőtheová was asked to resign from this, it still shows the potential for abuse of the GDPR.[84] Watching the kinks unfold after the enactment of the GDPR, the United States could perhaps consider an exemption for published journalism works to avoid the same censorship concerns in drafting its own comprehensive data privacy legislation.[85]

IX. CONCLUSION

The TikTok case has demonstrated the limitations to CFIUS, a committee that was often viewed as a black box, on the ability to regulate foreign companies. In the overarching war on Chinese apps, TikTok was poised to be just a piece in a much larger puzzle to eradicate Chinese companies from U.S. devices and app stores. From TikTok, the case reinforces that CFIUS may only act on "covered transactions". For TikTok, that "covered transaction" would have only included the U.S. assets that were acquired by ByteDance from Musical.ly and subsequently integrated in what makes today's TikTok.[86] Therefore, ordering a divestiture of TikTok in its entirety was an overextension of CFIUS's authority.

While taking the CFIUS avenue might work for regulating a narrower pool of foreign companies, this leaves a massive gap in the United States' ability to regulate and protect the personal data of American citizens. In the absence of comprehensive federal data privacy laws, the United States has been failing to regulate and protect its citizens' personal data. Comparatively, the European Union recently passed the GDPR, which has allowed its member states to take an entirely different approach to protecting the personal data of E.U. citizens. The GDPR is applicable to any company collecting and processing personal data of those citizens, rather than the "whack-a-mole" approach the United States has been taking with Chinese mobile app companies.[87] The United States is long overdue for a general data privacy regulation—the GDPR could serve as a model to the United States, taking lessons learned to build and enact an even better federal legislation of its own.

[1] "Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation." *Big Data*, GARTNER GLOSSARY, https://www.gartner.com/en/information-technology/glossary/big-data (last visited Mar. 9, 2021).

[2] *See* Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019), https://www.wired.com/story/wired-guide-personal-data-collection/ (describing the various and broad ways in which companies collect and use personal data).

[3] Fan Liang et. al., *A Survey on Big Data Market: Pricing, Trading and Protection*, IEEE ACCESS 6, 15133 (2018).

[4] Matt Day, *You're Home Alone With Alexa. Are Your Secrets Safe?,* BLOOMBERG (Dec. 31, 2019), https://www.bloomberg.com/news/articles/2019-12-31/you-re-home-alone-with-alexa-are-your-secrets-safe-quicktake.

[5] Ashley Carman, *AccuWeather deflects blame after selling users' data, even if they opt out*, THE VERGE (Aug. 24, 2017), https://www.theverge.com/2017/8/24/16197262/accuweather-app-mobile-sdk-collect-user-data-privacy.

[6] *See Waze – Privacy Policy,* WAZE, https://www.waze.com/legal/privacy#information-that-is-being-collected (last visited Nov. 15, 2020) (stating that, among other types of data collected, "detailed location, travel and route information" is collected).

[7] *Starbucks Privacy Statement*, STARBUCKS (last revised Aug. 18, 2020), https://www.starbucks.com/about-us/company-information/online-policies/privacy-policy#information_we_collect.

[8] *See* Carman, *supra* note 5 (describing how AccuWeather sells location data of users to Reveal Mobile, which uses the data to "understand the path of a consumer and where they go throughout the day"); *see also* Pierre-Yves Lanneau Saint Leger, *Waze, Crowd-Sourced Traffic App, Speeds Care to Crash Scenes but Shares Users' Personal Data*, TOOLBOX (July 16, 2019), https://www.toolbox.com/security/data-security/articles/waze-crowd-sourced-traffic-app-speeds-care-to-crash-scenes-but-shares-users-personal-data/ (describing how Waze sells location data to advertisers and can provide location data to police).

[9] "[S]ome of the solutions being proposed for TikTok — such as selling itself to American investors — wouldn't address the core problems. An American-owned TikTok could still legally sell data to third-party data brokers, for example, which could then feed it back to the Chinese authorities." Kevin Roose, *Don't Ban TikTok. Make an Example of It.*, N.Y. TIMES, https://www.nytimes.com/2020/07/26/technology/tiktok-china-ban-model.html (last updated Aug. 14, 2020).

[10] Sara Jeong, *The US Declared War On TikTok Because It Can't Handle The Truth*, THE VERGE (Aug. 7, 2020), https://www.theverge.com/21355465/tiktok-us-china-information-nationalism-online-propaganda.

[11] TikTok is a video sharing app, allowing users to create and share videos up to 60 seconds long. TikTok was formerly known as Musical.ly, which was founded in China. Musical.ly was then acquired by Chinese media and technology company ByteDance in 2017, which already had an app like Musical.ly, TikTok. The two were integrated to form the TikTok that we know of today. Heather Schwedel, *A Guide to TikTok for Anyone Who Isn't a Teen*, SLATE (Sept. 4, 2018), https://slate.com/technology/2018/09/tiktok-app-musically-guide.html.

[12] *See* Alexandra S. Levine, *The pandemic multiplied TikTok's audience – and its critics in Washington*, POLITICO (July 9, 2020), https://www.politico.com/news/2020/07/09/pandemic-tiktok-critics-washington-354467 (stating that TikTok's downloads peaked during the pandemic, surpassing 2 billion downloads, and also has seen a broadened user demographic).

[13] Michael Grothaus, *These were the most-downloaded apps of 2020 on Apple's App Store*, FAST COMPANY (Dec. 2, 2020), https://www.fastcompany.com/90581745/these-were-the-most-downloaded-apps-of-2020-on-apples-app-store.

[14] Levine, *supra* note 12.

[15] That same day, a second executive order was issued announcing a similar ban on Chinese mobile messaging app WeChat. Ana Swanson, *Trump's Orders on WeChat and TikTok Are Uncertain. That May Be the Point.*, N.Y. TIMES (Aug. 7, 2020), https://www.nytimes.com/2020/08/07/business/economy/trump-executive-order-tiktok-wechat.html; Bobby Allyn, *Trump's TikTok Sell-By Date Extended by 15 Days*, NPR (Nov. 13, 2020), https://www.npr.org/2020/11/13/933916944/trump-ordered-tiktok-to-be-sold-off-but-then-ignored-the-deadline#:~:text=Instead%2C%20on%20Friday%2C%20the%20Trump,U.S.%20over%20national%20security%20concerns.

[16] "A theory explaining all this has quietly and persistently circulated among TikTokers since the ban was first discussed a few weeks ago: What if this has nothing to do with China, nothing to do with national security? What if this does have everything to do with Trump's rally in Tulsa, Oklahoma, in June? The event was supposed to mark a

return to the campaign assemblies that the president covets, a comeback show of force with nearly 20,000 people in attendance after months of Covid 19 lockdown. And it was totally ruined for him by TikTokers and other young people online who coordinated a campaign to register for tickets to the event and never show up. So, what if the ban on TikTok is retaliation for that?" Abram Brown, *Is This The Real Reason Why Trump Wants To Ban TikTok?* FORBES (Aug. 1, 2020), https://www.forbes.com/sites/abrambrown/2020/08/01/is-this-the-real-reason-why-trump-wants-to-ban-tiktok/?sh=39a27a9f4aed.

[17] *See infra* Part II, Section B.

[18] *The Committee on Foreign Investment in the United States: Confidentiality,* U.S. DEP'T TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius#:~:text=CONFIDENTIALITY-,Section%20721%20of%20the%20Defense%20Production%20Act%20of%201950%2C%20as,Committee%2C%20subject%20to%20limited%20exceptions (last visited Feb. 14, 2021).

[19] Emily Birnbaum, *'This has been botched': This is what makes Trump's TikTok tirade so unusual*, PROTOCOL (Aug. 6, 2020), https://www.protocol.com/cfius-tiktok-not-how-this-works.

[20] Alex Sherman, *TikTok reveals detailed user numbers for the first time*, CNBC (Aug. 24, 2020), https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html.

[21] *See* Exec. Order No. 13,942, 85 Fed. Reg. 48637, 48637-48639 [hereinafter EO 13,942] (describing the authority to address the threat posed by TikTok as the IEEPA and the National Emergencies Act); *see also* Exec. Order No. 13,943, 85 Fed. Reg. 48641, 48641-48643 (Aug. 11, 2020) [hereinafter EO 13,943] (describing the authority to address the threat posed by WeChat as the IEEPA and the National Emergencies Act).

[22] EO 13,942, *supra* note 21 (Aug. 11, 2020); Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51297, 51297-51299 (Aug. 19, 2020).

[23] EO 13,942, *supra* note 21, at 48637.

[24] No TikTok on Government Devices Act, S. 3455, 116th Cong. (2020).

[25] *Id.*

[26] Regarding the Acquisition of Musical.ly by ByteDance Ltd., *supra* note 22.

[27] *Id.* at 21-22.

[28] *Id.* at 8.

[29] Kane Wu et. al., *China's ByteDance buying lip-syncing app Musical.ly for up to $1 billion,* REUTERS (Nov. 9, 2017), https://www.reuters.com/article/us-musical-ly-m-a-bytedance/chinas-bytedance-buying-lip-sync-app-musical-ly-for-up-to-1-billion-idUSKBN1DA0BN

[30] *Id.*

[31] Sarah Bauerle Danzman & Geoffrey Gertz, *Why is the U.S. forcing a Chinese company to sell the gay dating app Grindr?*, WASH. POST. (Apr. 3, 2019), https://www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr/.

[32] *Id.*

[33] Petition for Review at 8, TikTok Inc. v. Trump, Civil Action No. 1:20-cv-02658 (CJN) (D.D.C. Dec. 7, 2020).

[34] *Id.*

[35] Petition for Review, *supra* note 33, at 10.

[36] *Id.* at 9.

[37] *Id.* at 21-22.

[38] Paul Marquardt, *Unusual Tiktok Review Calls CFIUS Processes Into Question*, LAW360 (Aug. 7, 2020), https://www.law360.com/articles/1299589/unusual-tiktok-review-calls-cfius-processes-into-question.

[39] EO 13,942, *supra* note 21; Regarding the Acquisition of Musical.ly by ByteDance Ltd.,. *supra* note 22.

[40] *See generally* Marquardt, *supra* note 38.

[41] *Id.* at 21-22.

[42] Bob Davis et. al., *Trump Says U.S. Should Get Slice of Tiktok's Sale Price*, WSJ (Aug. 3, 2020), https://www.wsj.com/articles/trump-says-u-s-should-get-slice-of-tiktok-sale-price-11596479818.

[43] *Why we are suing the Administration*, TIKTOK (Aug. 24, 2020), https://newsroom.tiktok.com/en-us/tiktok-files-lawsuit.

[44] Petition for Review, *supra* note 33, at 18-19.

[45] *Id.* at 16.

[46] Joint Status Report at 1-2, TikTok Inc. v. Biden, Civil Action No. 1:20-cv-02658 (CJN) (D.D.C. Feb. 11, 2021).

[47] *See, e.g.*, Geoffrey A. Fowler, *Is it time to delete TikTok? A guide to the rumors and the real privacy risks*, WASH. POST. (July 13, 2020), https://www.washingtonpost.com/technology/2020/07/13/tiktok-privacy/ ("Privacy concerns have been the most viral aspect of the popular short-video social network in the last week."); *see also* Casey Bond, *Should You Delete TikTok? Experts Explain The App's Security Risks*, HUFFPOST (July 17, 2020), https://www.huffpost.com/entry/should-you-delete-tiktok-app-security-risks_l_5f10b32ec5b6cec246c0478f ("Ultimately, it's up to you to decide whether you're comfortable using an app that could be compromised by a distrusted foreign government.").

[48] *See e.g.* Kim Lyons, *Wells Fargo directs employees to remove TikTok from company mobile devices*, THE VERGE (July 11, 2020), https://www.theverge.com/2020/7/11/21320935/wells-fargo-bans-tiktok-devices-amazon-pompeo (stating that Wells Fargo instructed employees to remove TikTok from their company issued mobile devices).

[49] *Privacy Policy,* TIKTOK, https://www.tiktok.com/legal/privacy-policy?lang=en (last visited Nov. 9, 2020).

[50] Cookies involve automatic collection of user data outside of the app linked across all of the user's devices, however, cookies can be disabled if preferred. *Id. See e.g., Data Policy,* FACEBOOK, https://www.facebook.com/policy.php (last visited Nov. 9, 2020); *Twitter Privacy Policy,* TWITTER, https://twitter.com/en/privacy (last visited Nov. 9, 2020).

[51] *See Data Policy,* FACEBOOK, *supra* note 50 (noting that Facebook collects device signal information including nearby cell tower).

[52] Grace Tobin, *It's time to talk about TikTok and what it's doing with our kids' data*, ABC NEWS, https://www.abc.net.au/news/2020-02-19/should-we-trust-chinese-owned-tiktok-personal-data/11962086 (Feb. 18, 2020).

[53] Fowler, *supra* note 47.

[54] *Privacy Policy,* TIKTOK, *supra* note 49.

[55] Isobel Asher Hamilton, *As the US gets ready to ban TikTok downloads, there is still no proof the app is spying on you for China,* BUS. INSIDER (Sept. 18, 2020), https://www.businessinsider.com/tiktok-explainer-privacy-facebook-google-2020-7.

[56] Fowler, *supra* note 47.

[57] *Privacy Policy,* TIKTOK, *supra* note 49.

[58] Fowler, *supra* note 47.

[59] Charles Riley & Julia Horowitz, *Trump approves TikTok deal. Big questions remain*, CNN BUS. (Sept. 21, 2020), https://www.cnn.com/2020/09/21/tech/tiktok-oracle-walmart-explained/index.html.

[60] *Id.*

[61] *Id.*

[62] *See* James Palmer, *TikTok's Sale to Oracle Doesn't Fix Anything*, FOREIGN POL'Y (Sept. 16, 2020), https://foreignpolicy.com/2020/09/16/tiktok-sale-oracle-does-not-fix-anything-china-bytedance-trump/ ("The Oracle-ByteDance deal is yet another example of how Trump's fundamentally self-serving vision of the world makes him a dangerous ally.").

[63] Charlie Mitchell, *TikTok/WeChat executive actions fall short of data security and privacy needs, says former FCC security head,* INSIDE CYBERSECURITY (Sept. 22, 2020), https://insidecybersecurity.com/daily-news/tiktokwechat-executive-actions-fall-short-data-security-and-privacy-needs-says-former-fcc.

[64] *See* Robert McMillan, *Oracle Reports Breach With Micros Systems; Business-software maker requires users of point-of-sale systems to reset passwords, cites 'malicious code'*, WSJ (Aug. 8, 2016), https://www.wsj.com/articles/oracle-reports-breach-with-micros-systems-1470677095 (describing a breach to Oracle's Micros point-of-sale software by a Russian criminal gang in an attempt to steal payment-card data).

[65] Mitchell, *supra* note 63.

[66] *See* EO 13,942, *supra* note 21 (describing the authority to address the threat posed by TikTok as the IEEPA and the National Emergencies Act); *see also* EO 13,943, *supra* note 21 (describing the authority to address the threat posed by WeChat as the IEEPA and the National Emergencies Act); *see also* Hamilton, *TikTok Irish data center, supra* note 55.

[67] *See Forced sales are the wrong way to deal with Chinese tech*, ECONOMIST (Aug. 5, 2020), https://www.economist.com/leaders/2020/08/05/forced-sales-are-the-wrong-way-to-deal-with-chinese-tech (President Trump "has even suggested that the Treasury should get a cut for making the deal possible, a demand with no precedent").

[68] *Id.*

[69] *See* Jeremy Straub, *The U.S. has lots to lose and little to gain from banning TikTok and WeChat*, FAST COMPANY (Aug. 31, 2020), https://www.fastcompany.com/90545187/the-u-s-has-lots-to-lose-and-little-to-gain-from-banning-

tiktok-and-wechat ("In my view, these concerns could be better addressed by enacting national privacy legislation, similar to Europe's GDPR and California's CCPA, to dictate how data is collected and used and where it is stored.").
[70] Ben Wolford, *What is GDPR, the EU's new data protection law?*, GDPR EU, https://gdpr.eu/what-is-gdpr/ (last visited Sept. 26, 2020).
[71] 2016 O.J. (L 119) 83.
[72] *Statement: Intent to fine Marriott International, Inc more than €99 million under GDPR for data breach*, ICO (July 9, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/; *Intention to fine British Airways €183.39m under GDPR for data breach*, ICO (July 8, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/.
[73] A data subject is an "identified or identifiable natural person . . . an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" in the E.U. 2016 O.J. (L 119) 33.
[74] 2016 O.J. (L 119) 82.
[75] 2016 O.J. (L 119) 32-33.
[76] *Id.*
[77] *See* Natasha Lomas, *TikTok announces first data center in Europe*, TECHCRUNCH (Aug. 6, 2020), https://techcrunch.com/2020/08/06/tiktok-announces-first-data-center-in-europe/ (explaining that one way for companies to avoid the risk of violating the GDPR through transfers of personal data to third countries is to process European personal data in the European Union).
[78] *Id.*
[79] *See* Nani Jansen Reventlow, *Can the GDPR and Freedom of Expression Coexist?*, 114 AJIL UNBOUND 31, 31-34 (2020) (arguing that the GDPR limits the right to freedom of expression, especially in journalism); *see also* Roslyn Layton, *The 10 Problems of the GDPR*, AM. ENTER. INST. (Mar. 12, 2019), https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf (outlining some of the issues with the GDPR that the U.S. could avoid).
[80] Bernhard Warner, *Online-Privacy Laws Come With a Downside*, THE ATLANTIC (June 3, 2019), https://www.theatlantic.com/ideas/archive/2019/06/europes-gdpr-elevated-privacy-over-press-freedom/590845/.
[81] *Id.*
[82] *Id.*
[83] Nikolaj Nielsen, *EU data protection rules abused to censor media*, EU Observer (May 26, 2020), https://euobserver.com/justice/148454.
[84] *Id.*
[85] Although, a challenge may be presented because formally classifying who is a journalist these days is hard to do.
[86] Petition for Review, *supra* note 33, at 21-22.
[87] *Forced sales are the wrong way to deal with Chinese tech*, *supra* note 67.