TikTok v. Trump and the Uncertain Future of National Security-Based Restrictions on Data Trade

Bernard Horowitz* & Terence Check**

ABSTRACT

*Looking through the lens of the D.C. District Court's 2020 decision on President Trump's TikTok "ban" (*TikTok v. Trump*), this article assesses whether U.S. law can address national security concerns raised by cross border data trade while accommodating the needs of industry.*

The type of data valued by foreign rivals of the United States has gradually shifted in accordance with technological progress and geopolitical dynamics. During the 2000's and early 2010's, cyber-based foreign economic collection campaigns targeting the U.S. focused on high-value IP data and trade secrets. However, in the past few years, increasing societal reliance on the internet in tandem with advances in data processing and algorithms has produced a new type of data-related security concern: foreign adversarial mass bulk collection of quotidian U.S. person data, including biometric data (for example, facial photographs). The apparent threat posed by foreign mass collection of such data – which has been publicly and prominently emphasized by the U.S. Intelligence community ("IC") – gives rise to a philosophical conflict. On one hand, the IC and privacy advocates regard foreign adversarial access as a threat. On the other hand, business interests have grown heavily reliant on data trade. In some industries, such as the music business in the streaming era, data collection and trade may be pivotal to profitability and growth. TikTok, which originally began as a music-sharing platform, is alone worth $400 billion.

Reconciling these opposing priorities and formulating a policy solution to such foreign data collection appears difficult under existing U.S. legal authorities. For example, the International Emergency Economic Powers Act ("IEEPA") and the Committee on Foreign Investment in the United States ("CFIUS")—under which foreign access to data might be restricted—may not be cleanly applicable to this cross-border data trade.

---

* Law Clerk for Senior Judge Mary Ellen Coster Williams of the United States Court of Federal Claims. This article does not reflect the views of the Court of Federal Claims or Judge Williams, and was written solely in the author's personal capacity and not as part of his court-related duties.

** Senior Counsel, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security; LL.M in Law & Government, specializing in National Security Law & Policy, American University Washington College of Law (2015); J.D., magna cum laude, Cleveland State University, Cleveland-Marshall College of Law (2014); Editor-in-Chief, *Cleveland State Law Review* (2013-2014). This article does not reflect the official position of the U.S. government, DHS, or CISA and all opinions expressed are solely those of the authors. The authors would like to thank friends and advisors who provided much-appreciated input on this article, including Prof. Sandra Aistars, Ethan Baer, Thomas Christian, Prof. James Cooper and Prof. Jeremy Rabkin.

IEEPA, which is the main U.S. framework for sanctions, has been traditionally applied to dictatorships and rogue regimes in response to terrorism sponsorship, weapons proliferation, slavery, corruption, war crimes, and genocide. Even though foreign collection of quotidian U.S. person data poses national security liabilities, the invocation of such a powerful legal mechanism as a response to bulk data collection may not be considered proportional or reasonable. Beyond this, the IEEPA statute (passed in 1977) forecloses sanctions prohibiting or constraining "personal communication[s] which do not involve a transfer of anything of value" or the exportation of "informational materials." The D.C. District Court's 2020 ruling in TikTok v. Trump *construed quotidian U.S. data and TikTok content as falling within this language; thus, the applicability of IEEPA to restricting data trade on national security grounds appears legally uncertain.*

Likewise, CFIUS—the framework for screening foreign adversarial investments in U.S. companies—does not appear to represent a full solution to regulating foreign adversarial access to quotidian U.S. data. CFIUS was expanded between 2018-2020 to theoretically cover foreign minority stake investments giving rise to U.S. data collection. However, in any case, U.S. federal law widely permits the selling of data, and this is reflected in the emergence of a lucrative data brokerage industry. A foreign party seeking U.S. data may not need to invest in a company if it can simply buy such data from a broker. Furthermore, the Federal Trade Commission—responsible for keeping an eye on data trade in practice – does not appear to have a relationship with CFIUS and disclaims a "national security"-related role.

In short, TikTok v. Trump *traces a challenging reality: even though constitutional law (*Dames & Moore v. Regan*) confers overwhelming authority on executive branch administrative national security mechanisms such as IEEPA and CFIUS, the applicability of these frameworks to properly regulate foreign bulk data collection, including some highly sensitive personal data, has proven unclear. Additional new legislation may be necessary to balance security concerns with private sector interests in unrestricted data trade.*

INTRODUCTION

For a few months in 2020, a legal fight over the future of social media and the video sharing app TikTok—whose parent company, ByteDance, is based in China—radiated out from the arcane confines of trade and national security law and into broader public discourse. President Donald Trump used his International Emergency Economic Powers Act ("IEEPA") authorities to issue Executive Order 13942 prohibiting TikTok-related transactions and ordering a ban on future downloads.[1] TikTok soon brought suit in the United States District Court for the

1. Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020).

District of Columbia to enjoin the download bans and other actions required in the Executive Order from taking effect.[2] The court ruled in favor of TikTok, holding that the President's order exceeded his IEEPA authorities because (1) TikTok's data transmissions constituted "personal communications which do[] not involve anything of value" and (2) TikTok content amounted to protected "informational materials."

The D.C. District Court's landmark suspension of an IEEPA Order illustrates two key challenges for the U.S. government and the technology industry—one regulatory and the other philosophical. The regulatory challenge is the reality that the legal framework governing data privacy and trade is outdated, impairing the capacity to manage the liabilities of foreign collection of quotidian U.S. person data; such data ranges from straightforward personal information, like names and dates of birth, to highly sensitive biometric data, such as facial photographs. The philosophical challenge entails a conflict between the incentives of the U.S. private sector on one hand and the national security establishment on the other: the private sector benefits from unrestricted cross-border data trade, while national security and privacy concerns lead government stakeholders to seek restrictions on foreign adversarial access to such data.

Irrespective of these clashing priorities, the *TikTok* court's central holding that social media data amounts to "personal communication[s] which does not involve a transfer of anything of value,"[3] which thus fall outside the scope of IEEPA, so severely misaligns with the reality of data value and commerce that this reasoning may be regarded as an unstable liability from *all sides* of this philosophical debate. In other words, a national security hawk who favors barring Chinese access to U.S. person data might hungrily regard the court's reasoning as easily reversed or circumvented with legislation or additional executive action. Likewise, business interests eager to engage Chinese markets should be wary that while the *TikTok* decision is nominally sympathetic, its legal rationale is at least partially unstable.

Both theoretical positions have merit. Proponents of restricting foreign data access can point to clear national security threats from such access: China's foreign economic competition against the United States has been prolific for more than a decade.[4] China's intense focus on artificial intelligence casts once ordinary data transfers in new light because the sophistication of algorithm technology—used to sort and synthesize data—has also been progressing dramatically.[5] In 2018, the U.S. Intelligence community issued public warnings about the dangers

2. TikTok v. Trump, 507 F. Supp. 3d 92, 98 (D.D.C. 2020).

3. *See* 50 U.S.C. § 1701(b)(1).

4. *See, e.g.*, OFF. OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE (2011), https://perma.cc/JJE9-4MXK.

5. For example, already in 2012, the ABA Standing Committee on Law and National Security's FISA Task Force discussed a potential future amendment (carve-out) to FISA whereby the probable cause standard for a FISA order (probable cause that a surveillance target is an agent of a foreign power) could be established based exclusively on computerized algorithmic synthesis of open source data. American Bar Association Standing Committee on Law and National Security: FISA Task Force

of regular social media data in the hands of U.S. adversaries.[6] The *TikTok* litigation itself corroborates the overwhelmingly wide scope of TikTok's collection and dissemination through TikTok's own Terms of Service ("TOS"), and also the contractual agreement between ByteDance, TikTok's Chinese parent company, and the Chinese Communist Party ("CCP").[7]

Furthermore, while we were drafting this article, TikTok announced new expansions to their data collection practices, this time focusing on the biometric data of its users.[8] There should be little doubt that such information is used by the CCP to assemble individualized user profiles, since this is already the practice of Western tech companies.[9] The national security implications will only grow more intense. In June 2021, President Biden issued Executive Order 14034, rescinding the "ban" on TikTok and directing a number of national security-oriented departments and agencies to review, using a series of criteria, whether certain apps from adversarial nations posed a national security risk to U.S. citizens' data.[10] While the Trump and Biden administrations may diverge on the specific question of whether to ban TikTok at this moment, observers could conclude that a keen federal national security interest in foreign data exports has endured the change in power in Washington. Further evidence of this can be found in the relatively new Department of Commerce reviews of information and communication technology services ("ICTS"), which has arisen during the drafting of this article and, for the sake of brevity and expediency, falls outside this article's scope.

For the private sector, the stakes of cross-border data restrictions are likewise high and extraordinarily high for industries whose business models and profit margins now hinge on data trade and circulation as a critical part of their bottom lines. To illustrate, the big data era has witnessed the emergence of an entire data broker industry;[11] at least some areas of the private sector now rely heavily on the data economy to remain substantially profitable. For example, recording industry profits declined by sixty-six percent between 2000 and 2012 due to online file sharing and the related obsolescence of physical sales of CD's and LP's; while the music business has partially recuperated by pivoting to streaming, streaming

Meeting at Morgan Lewis (Jan. 6, 2012); American Bar Association Standing Committee on Law and National Security: Meeting at Morgan Lewis (Oct. 3, 2012).

6. *See*, *e.g.*, Sara Salinas, *Six Top US Intelligence Chiefs Caution Against Buying Huawei Phones*, CNBC (Feb. 13, 2018, 11:03 AM), https://perma.cc/G2SZ-3H5Z.

7. TikTok v. Trump, 507 F. Supp. 3d at 95.

8. Sarah Perez, *TikTok Just Gave Itself Permission to Collect Biometric Data on US Users, Including 'Faceprints and Voiceprints'*, TECHCRUNCH (June 3, 2021, 11:57 PM), https://perma.cc/B6N8-VPJQ.

9. *See, e.g.*, Davis v. Facebook, Inc. (*In re Facebook, Inc. Internet Tracking Litig.*), 956 F.3d 589, 595 (9th Cir. 2020) ("Facebook uses plug-ins to track users browsing histories when they visit third-party websites, and then compiles these browsing histories into personal profiles which are sold to advertisers to generate revenue.").

10. Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021).

11. Michael Kans, *Data Brokers and National Security*, LAWFARE (Apr. 29, 2021, 8:01 AM), https://perma.cc/E34P-R9CF; *see also* Alfred Ng & Maddy Varner, *The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress*, MARKUP (April 1, 2021, 8:00 AM), https://perma.cc/79Z2-GCEA.

revenue does not approach that previously achieved by physical sales. This amplifies the financial necessity of maximizing collateral sources of recording-derived revenue, which hinge on data trade.[12] Even beyond the potential business gains and losses depending on the ease of data trade, there also remains a Cold War-derived national security argument about the ultimately desirability of circulating information from the West into non-democratic countries to showcase democratic values.[13] For example, Mandiant's landmark 2013 investigation of Chinese foreign economic collection campaigns against the West indicated that the Chinese hackers were fervent Harry Potter fans.[14]

As we describe below, addressing these data trade and security issues within existing legal frameworks could either fail to resolve the issue (as in the case of export controls or CFIUS reviews) or could grievously injure the economic interests of the telecom and recording industry. So, ultimately, the clash between these conflicting priorities—(A) proponents of national security-based restrictions on data transactions and circulation and (B) private sector free market advocates—will be fought on a battlefield of U.S. regulatory law which is outdated and seems to point in the direction of reform through legislation.

Part one of this article is a survey of seemingly applicable administrative law mechanisms that the U.S. government could use to regulate data exports through apps like TikTok. These include IEEPA, CFIUS, the Federal Trade Commission ("FTC") Act of 1914, and the governing Supreme Court decision tracing the extent of executive power in this area, *Dames & Moore v. Regan*.

Part two of this article is an overview of how foreign adversarial bulk data collection has emerged as a threat over time. We focus on this emergence because the *TikTok* decision contends that sensitive personal data, including biometric data, is not sufficiently valuable to warrant IEEPA's protection. We examine the

12. Some legal experts believe that anti-trust and data privacy interests may be inconsistent with each other, speculating more competition in the data industry, where lots of companies hold lots of data, may have worse implications for privacy than one or two extremely large companies. These experts also think that busting trusts might lead to an opening for foreign investment, allowing Chinese companies to buy up the carved up bits of American companies, though these same experts may believe that existing models, such as CFIUS, might close the gap. The Cyberlaw Podcast, *Episode 368: The Trustbusters Come for Big Tech*, STEPTOE AND JOHNSON, at 08:00–17:13 (June 28, 2021), https://perma.cc/MS8T-R2DZ. But, as we discuss below, CFIUS pertains only to ownership interests in companies, not to sales of goods or commodities like personal data. If antitrust legislation or enforcement measures would lead to the break up of American social media companies, this would create a major growth opportunity for Bytedance, which owns social media platforms TikTok and Douyin. The latter app exists only in China, and combined with TikTok, gives Bytedance 1.9 billion users. *TikTok Is Rolling out Longer Videos — but the Real Story Is Its Chinese Sister Douyin*, ROBINHOOD SNACKS (July 2, 2021), https://perma.cc/3A7E-S6ZY.

13. North Korea provides an extreme example of this idea, where tyrannical crackdowns on outside influence can lead to lengthy prison sentences for watching a Chinese film or even death for possessing foreign media content. Laura Bicker, *Why Kim Jong-un Is Waging War on Slang, Jeans and Foreign Films*, BBC (June 7, 2020), https://perma.cc/B6EM-5BK4. *See also* Jay Newton-Small, *Hillary's Little Startup: How the U.S. Is Using Technology to Aid Syria's Rebels*, TIME (June 13, 2012), https://perma.cc/H6F5-KAUZ.

14. Christopher Bodeen, *Badminton, Harry Potter and Facebook: A Look at Chinese Unit Accused of Huge Hacking Operation*, GLOB. NEWS CAN. (Feb. 20, 2013, 12:51 AM), https://perma.cc/54QN-S469.

biometric data field in particular, given its recent prominence in societal discourse, high importance for authentication, and ultimate irreplaceability as our key area of focus.

Part three discusses the D.C. District Court's *TikTok v. Trump* decisions in detail. The case establishes the reality that unfortunately, two subsections of IEEPA cripple application of this framework for foreign bulk collection of quotidian data. *TikTok v. Trump* is also a decision that implausibly construes data as "personal communication[s] which does not involve a transfer of anything of value," i.e., as immune from IEEPA sanctions. This Part discusses how such data does have both economic and security value, setting up the collision we anticipate in Part four of this article.

Part four draws on our analysis of *TikTok v. Trump* by examining industry and consumer stakes underlying data regulation/restriction disputes. This Part also appraises legislative efforts to address the issue of data exports to adversarial nations.

Part five illustrates one prominent example of how significant restrictions on data trade could impact industry: for the music business, the rise of the data economy has enabled newfound growth, and an escape from years of economic turmoil.

This article will hopefully aid national security practitioners in understanding the legal backdrop of the risks associated with cross-border data transfers (particularly of biometric data), identifying shortfalls in current laws and regulations, and formulating new ways to further national and economic security while ensuring personal privacy by ensuring responsible handling of biometric information. We also hope to assist state lawmakers looking to identify new data privacy risks, industry counsel advising their clients on such transfers, and the general public trying to make educated decisions about their consumer choices in a complex information economy.

PART 1: ADMINISTRATIVE NATIONAL SECURITY LAW MECHANISMS APPLICABLE TO RESTRICT FOREIGN BULK DATA ACCESS

Even though U.S. federal law largely reflects a laissez-faire approach to data trade and privacy friendly to business and innovation, the U.S. government has available several legal frameworks aligning with national security risks posed by exports of personal data to foreign adversaries.[15] We consider whether these frameworks—separately or collectively—can address national security threats while also balancing the private industry needs for flexibility and room to innovate.

15. Karen Schuler, *Federal Data Privacy Legislation Is on the Way – That's a Good Thing*, IAPP (Jan. 22, 2021), https://perma.cc/TGZ4-BWEV.

A. IEEPA

The International Emergency Economic Powers Act ("IEEPA") emerged in 1977 to succeed the "Trading with the Enemies Act" ("TWEA"). TWEA had been passed by Congress during the lead-up to U.S. involvement in World War I, empowering the President to declare "national emergencies" through which basic communications and financial intercourse with "enemies" of the United States could be restricted.[16]

Shortly after assuming office in 1933, President Roosevelt appealed to Congress to invoke TWEA, not with respect to a foreign adversary, but rather toward the Great Depression. Roosevelt requested "broad executive power to wage a war against the emergency, as great as the power that would be given to me if we were in fact invaded by a foreign foe."[17] Receiving the support he sought, Roosevelt declared a "bank holiday" and suspended all financial transactions at all U.S. banking institutions for a period of four days.[18]

Four decades later, the Church and Pike Committees investigated U.S. Intelligence community activities (and perceived excesses) in the aftermath of the Nixon administration, Watergate, and the death of FBI Director J. Edgar Hoover. IEEPA was one step in the flurry of legislation which followed. The Church Committee scrutinized TWEA, observing that under the Roosevelt "emergency," the United States had been in an emergency state since March 9, 1933.[19] Reviewing TWEA, wary of excessive executive power without congressional checks, the Committee recognized four problems: (1) TWEA did not require consultations or reports to Congress about declarations of national emergencies or use of the powers therein, (2) TWEA-based emergency declarations had no time limits, no mechanisms for congressional review, and no means by which Congress could terminate an emergency if it disagreed, (3) TWEA did not set limits on the "emergency" economic powers available to the President and on the circumstances under which such powers might be exercised, and (4) actions taken under the authority of TWEA often were unrelated to the national emergency declared.[20]

Congress thereby moved to remedy the flaws in TWEA with IEEPA. IEEPA's main improvement on TWEA is an oversight mechanism for the declaration of national emergencies: namely, the National Emergencies Act ("NEA"). To enable IEEPA powers, the President must declare an emergency under the NEA through an Executive Order.[21] Emergency declarations require the President to "immediately" issue a proclamation to Congress, which must be published in the

16. CHRISTOPHER A. CASEY, IAN F. FERGUSSON, DIANNE E. RENNACK & JENNIFER K. ELSEA, CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION AND USE (2020), https://perma.cc/2Y5J-AHLH at 3.

17. *Id.* at 4.

18. *Id.*

19. *Id.* at 6-7.

20. *Id.* at 7-8.

21. 50 U.S.C. §§ 1701–1708.

Federal Register.[22] However, aside from the required proclamation, the power to declare an "emergency" under the Act is broad – the President may even declare an "emergency" under the Act when his own actions have intentionally given rise to the "emergency."[23] Originally, the NEA included a legislative veto so that Congress could move to terminate national emergencies with a concurrent resolution. After the Supreme Court declared such vetoes unconstitutional,[24] Congress amended the NEA to require a joint resolution to overturn NEA emergency declarations. Only two such resolutions have ever been introduced, and neither case involved an IEEPA order.[25]

Under IEEPA, having declared an emergency, the President (or an executive branch entity to which the President delegates power) may "investigate, regulate, or prohibit"[26] foreign financial activity within the United States posing a threat to U.S. national security, foreign policy, or economic interests. This includes the power to take control of "any property in which any foreign country of a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States."[27]

Thus, the economic measures available under IEEPA to restrict foreign economic activity are nearly limitless, and include the capacity to impose sanctions, freeze assets, and force sales of companies.[28] These responsibilities customarily fall to the Office of Foreign Asset Control ("OFAC") within the Treasury Department.

However, IEEPA does include a caveat, namely, specifying types of activity which may *not* be prohibited through sanctions. The statute, as amended, reads in part:

> The authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly—
> 1. any postal, telegraphic, telephonic, or other **personal communication, which does not involve a transfer of anything of value**; [emphasis added]
>
> 2. [. . .]
>
> 3. the importation from any country, or exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, **of any information or informational materials**, including but not limited

22. 50 U.S.C. § 1621.

23. *See* Robert Chesney, *You Are "Hereby Ordered" To Listen to This Podcast*, NAT'L SEC. LAW PODCAST (Aug. 28, 2019), https://perma.cc/F8X3-6TME at 13:30-15:00.

24. I.N.S. v. Chadha, 462 U.S. 919 (1983).

25. "Two such resolutions have ever been introduced and neither declarations of emergency involved IEEPA. The lack of congressional action here could be the result of the necessity of obtaining a veto-proof majority or it could be that the use of IEEPA has so far reflected the will of Congress." CONG. RSCH. SERV., *supra* note 16, at 46.

26. 50 U.S.C. § 1702(a)(1)(A).

27. 50 U.S.C. § 1702(a)(1)(B).

28. 50 U.S.C. § 1702(a)(1)(A)–(B).

> to, publications, films, posters, phonograph records . . . CD ROMs . . . and news wire feeds.[29] [emphasis added]

It is apparent from these exceptions in 50 U.S.C. § 1702(b) that even amidst intense disputes with adversarial countries (for example, the USSR in 1977), Congress sought to prevent the President from restricting personal communication and the flow of information. On the surface, this carve-out is easy to understand – during the Cold War, Western openness was seen as an antidote to Communist totalitarianism.[30]

However, beyond this, the legislative history of IEEPA—specifically the House International Relations Committee hearings concerning section 1702(b) (beginning on March 29, 1977)—tells a more nuanced and enlightening story. In the aftermath of the Church Committee hearings and Watergate, Congress passed the Foreign Intelligence Surveillance Act ("FISA") to integrate national security surveillance into the federal court system. FISA was introduced in the Senate in May 1977 and eventually signed into law in October 1978. Overlapping this period, in July 1977, the House International Relations Committee was concerned that under TWEA (or IEEPA as contemplated), the President could order surveillance (wiretapping or interception of regular mail) through a declared "emergency." Therefore, IEEPA – specifically 50 U.S.C. § 1702(b)(1) – was at least partially based on closing a perceived loophole for ordering warrantless surveillance.[31]

A lawyer for OFAC, Leonard Santos, testified before the Committee in 1977 and raised concerns about the 1702(b) carve-outs. Santos explained that he and his department did not object to the expressed policy aims (i.e., creating checks and balances for National Emergency economic powers by replacing TWEA with IEEPA), but had specific concerns about the *language* of 1702(b). In response to Santos, R. Roger Majak, the Committee's Staff Director, confirmed on the record that 1702(b) "[is] admittedly, a very difficult area to draft and we have some difficulty with that section."[32]

Santos warned that as drafted, 1702(b) would prevent IEEPA from being applied to bar putative "communications" which were actually financial transactions tied to countries adverse to the United States:

> On page 8, Mr. Chairman, section (b)(1). **We are troubled by the phrase, "which does not involve the transfer of anything of value." We are not**

29. 50 U.S.C. § 1702(b).

30. Radio Free Europe/Radio Liberty, a U.S. government media agency with independent editorial control over content, provides an enduring example of this policy idea. Conceived in the early days of the Cold War and continuing today in dozens of languages, Radio Free Europe/Radio Liberty brings independent journalistic content to totalitarian countries with information-poor environments. *History*, RADIO FREE EUR./RADIO LIBERTY, https://perma.cc/9JXU-KG4Y.

31. *Hearings on H.R. 1560 and H.R. 2382 before the Subcomm. on Int'l Econ. Pol'y & Trade of the Comm. on Int'l Rels.*, 95th Cong. 195–201 (1977).

32. *Id.*

> **sure that includes any form of commercial transaction. It permits, someone noted, the mailing of a contract. While it might not be of value, in a certain sense, it might nonetheless be something we may wish to inhibit. These uncompensated transfers of anything of value, the conditions that are imposed by that struck us as not adequate.**
>
> . . . **we are not sure that [1702(b) as drafted] necessarily covers commercial transactions, all commercial transactions.** What we are getting at here, frankly – there is certainly no objection, I doubt seriously whether there [are] any objections and nobody has ever expressed an objection to genuine postal, telegraphic, telephonic or other personal communication. Nobody really questions that. What we really question is, if those words could be used to cover other activities that we think could legitimately be the subject of interference under (5)(b). **What we would like to be sure of is that this language does not permit subterfuge, does not permit people to use the postal system to transfer things, even if they are not of value but may be a subject of legitimate prohibition.**
>
> The only point we are trying to make is that we are uncomfortable with these exceptions not because we not in favor of the general purpose involved, but we hope that careful language could be worked out that would prohibit subterfuge one way or the other.[33] [emphasis added]

At least outwardly, Members of the Committee were receptive to Santos's warning that while he had no quarrel with Congress's legislative aims, 1702(b) as drafted would prevent OFAC from using sanctions to stop transactions connected with adversarial foreign countries passing as putative "communications," amounting to "subterfuge." Representative Jonathan Bingham of New York, the Chairman of the Committee, concluded matters by suggesting that Santos's concerns be referred for further work:

> Mr. Bingham: Let us go on. I think that we ought to identify those areas of substantive difference and then get the subcommittee members here to express their opinions. We will try to arrive at a consensus on the substance; then we can leave it to the staff working with Mr. Santos and his associates to see if satisfactory language can be worked out. We have identified several substantive questions . . . I would propose, if there is no objection, that we agree for the purpose of referral to the full committee, that we will leave in the exemptions in some form and ask the staff to see if they can work out precise language to meet the price objections of the administration.[34]

Unfortunately, Santos's warning about the draft language of 1702(b) did not lead to any further revisions of the language as drafted, and the issue surfaced

33. *Id.*
34. *Id.*

almost verbatim, forty-three years later, in *TikTok v. Trump*. We further discuss below in Part 3 how Santos's views expressed at the time prophesied the current problem.

B. CFIUS

The Committee on Foreign Investment in the United States ("CFIUS") conducts national security reviews of foreign investments in U.S. businesses. CFIUS has evolved dramatically since it was created through an Executive Order in 1975. The Committee stands empowered today largely because of U.S. economic competition with Japan in the 1980's, a period when Japan moved to strategically weaken and then purchase U.S. companies enmeshed with the U.S. Defense Industrial Base ("DIB"), arousing the concern of the defense establishment and Intelligence community.

In 1983, a Japanese company tried to acquire a U.S. steel manufacturer,[35] and the Department of Defense responded by classifying the metal compositions being developed by the manufacturer, forcing the Japanese firm to withdraw from the planned purchase.[36] In 1985, a Japanese company attempted to acquire a U.S. company which manufactured ball bearings (subcomponent parts used in wheels) for the U.S. military – the agreement was completed only after the Japanese company agreed to keep the manufacturing operations inside the United States.[37]

However, with no formal process or authority for navigating such sensitivities, the issue finally came to a head in March 1987 when Fujitsu, a Japanese IT company, moved to purchase Fairchild Semiconductor. The Department of Defense, the Commerce Department, and the Central Intelligence Agency collectively raised strong objections with the White House, and the dispute became public.[38] Fairchild, which manufactured computer chips and held many U.S. defense contracts, was reportedly losing money because Japanese companies were selling similar computer chips at lower prices in the United States; this was part of a purported Japanese economic strategy to flood the computer chip market, weaken American companies and then purchase those companies, so as to control the entire semiconductor market and the supply chain by leaving no major semiconductor manufacturer owned by the United States.[39] According to the *New York Times*, DoD and CIA officials warned that if the deal were allowed, "the American computer industry would become dependent on semiconductors produced by Japanese-owned manufacturers."[40] However, what must have surprised

35. JAMES K. JACKSON, CONG. RSCH. SERV., RL33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 6–7 (2020), https://perma.cc/42V7-YED5.

36. *Id.*

37. *Id.*

38. David E. Sanger, *Japanese Purchase of Chip Maker Canceled After Objections in U.S.*, N.Y. TIMES (Mar. 17, 1987), https://perma.cc/6KNQ-3BC4.

39. *Id.*

40. *Id.*

policy makers most was that "the government had no means of preventing the acquisition."[41]

CFIUS became those means. The constitutional arrangement that enables CFIUS (under the Exon-Florio Amendment of 1988) relies on a congressional delegation to the executive branch of Congress's foreign commerce power ("Commerce with foreign Nations") under Article 1, Section 8 of the Constitution.

Thus equipped by Congress, the President is empowered to "suspend or prohibit any **covered transaction** that threatens to impair the national security of the United States."[42] These powers become available when "**credible evidence** . . . leads the President to believe that the foreign interest exercising control [in a given covered transaction] might take action that threatens to impair the national security."[43] The President's decision is ultimately guided by a list of factors identified in the CFIUS statute which trace the national security implications of such transactions.[44]

The baseline jurisdiction of CFIUS – which regulates "covered transaction[s]" – is extraordinarily broad. "Covered transactions" include "any merger, acquisition or takeover that is proposed or pending after August 23, 1988 [(the date of the Exon-Florio Amendment)], by or with any foreign person that could result in foreign control of any **United States business**,[45] including a merger, acquisition or takeover carried out through a joint venture."[46]

The 2018 Foreign Investment Risk Review Modernization Act (FIRRMA) expansion of CFIUS attempts in part to bridge the gap between the CFIUS mission and cyber-based national security vulnerabilities, especially including access to sensitive information via foreign investments (directly or indirectly). According to law firms citing insiders, once the United States began limiting and policing foreign "controlling" investments in U.S. companies (i.e. CFIUS looking for investments yielding sufficient foreign ownership to exert direct control over a company), foreign adversaries seeking access to sensitive U.S. data pivoted toward using minority, non-controlling investments which facilitate quiet access to sensitive and valuable data.[47] While such minority investments may not include corporate voting rights, minority investors often have the ability to ask for favors or influence key decisions: for example, arranging for the company to hire key

41. *Id.*

42. 50 U.S.C. § 4565(d).

43. 50 U.S.C. § 4565(d)(4) (50 U.S.C. app. 2170 (1988)).

44. 50 U.S.C. § 4565(f).

45. "United States business" includes any foreign business operating in U.S. interstate commerce—therefore, CFIUS jurisdiction includes foreign transactions resulting in U.S. commerce. *Cf.* Dubai Ports case (reviewing UAE entity's purchase of a British company doing business in the United States). 50 U.S.C. § 4565(a)(13).) *See* David E. Sanger, *Under Pressure, Dubai Company Drops Ports Deal*, N.Y. TIMES (Mar. 10, 2006), https://perma.cc/WH53-R3PU.

46. 50 U.S.C. § 4565(a)(4)(B)(i).

47. J. Dormer Steven & Alfredo G. Fernandez, *Expansion of CFIUS Oversight of Certain Non-Controlling Foreign Investments*, SHIPMAN & GOODWIN LLP (Dec. 11, 2018), https://perma.cc/G8N2-VSR2.

management personnel with access to protected data, or subtly guiding the strategic decisions of the company.[48] FIRRMA was passed to address such access contingencies, and against a backdrop of intense China-US trade tensions (inflamed by COVID).

Accordingly, FIRRMA critically expanded CFIUS jurisdiction to additionally include certain foreign minority, *non-controlling* investments ("other investments") in U.S. businesses potentially enabling foreign actors to access and steal sensitive data.

The pertinent innovation in FIRRMA is the "other investments" framework – designed to scrutinize minority, non-controlling investments posing possible data theft risks. The "other investments" CFIUS trigger entails a two-part test: (1) the reviewed foreign investment must be made in a U.S. "**TID**" (technology, infrastructure or data) **business** and (2) the foreign investment must provide the investor with **access-related rights**.[49] Hence, the test asks: (1) is this company a target for foreign collection and (2) does the investment arrange access to protected information or data?

"TID Business" is defined in statute as including any company (A) involved with critical infrastructure, (B) working with "critical technologies" or (C) maintaining or collecting sensitive personal data of United States citizens that may be exploited in a manner that threatens national security.[50] Notably, the definition of "critical technologies" fully blankets all imaginable contingencies in which sensitive data or data technology may be at stake.[51]

Access related rights entail:

1. The ability to access any material nonpublic technical information[52] in the possession of the TID Business;
2. The right to nominate a member or observer to the board of directors of the TID U.S. Business; or
3. Any involvement, other than through voting of shares, in the substantive decision-making of the TID U.S. Business regarding—

48. PricewaterhouseCoopers, *A Practical Guide to IFRS – Consolidated Financial Statements* 8 (July 2011), https://perma.cc/HSF4-QFU4.

49. 50 U.S.C. § 4565(a)(4)(B)(iii), (a)(4)(D)(i).

50. *See* 50 U.S.C. § 4565(a)(4)(B)(iii).

51. *See* 50 U.S.C. § 4565(a)(6)(vi) (construing "emerging and foundational technologies" as "critical technologies" and noting that identification of "Emerging" and "Foundational" technologies turns on Federal Register Notices filed by the Department of Commerce's Bureau of Industry and Security (BIS)); *see* Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (Nov. 19, 2018); *see also* Identification and Review of Controls for Certain Foundational Technologies, 85 Fed. Reg. 52,934 (Aug. 27, 2020).

52. Definition of "material nonpublic technical information":

> [Information which either] (A) "provides knowledge, know-how, or understanding, not available in the public domain, of the design, location, or operation of critical infrastructure"; or (B) "is not available in the public domain, and is necessary to design, fabricate, develop, test, produce, or manufacture critical technologies, including processes, techniques, or methods." 50 U.S.C. § 4565(a)(4)(D)(ii).

a. the use, development, acquisition, safekeeping or release of **sensitive personal data** of US citizens maintained or collected by the US business
b. the use, development acquisition, or release of critical technologies; or
c. the management, operation, manufacture, or supply of critical infrastructure[53] [emphasis added]

"Sensitive personal data," defined under FIRRMA, includes not only national security data, but also U.S. person data generally – business data practices which: (1) target or tailor products or services, such as to U.S. government personnel, (2) maintain or collect data on more than 1 million individuals, or (3) have a demonstrated objective to maintain or collect data on more than 1 million individuals as part of a product or service.[54]

Hence, in short, FIRRMA widened CFIUS to guard against minority, non-controlling foreign investments enabling foreign bulk data collection against U.S. persons or establishing access to sensitive data because of its substantive value.

C. Foreign Adversarial Data Access and Circulation: CFIUS and the FTC

Unfortunately, the CFIUS-FIRRMA framework as applied to national security-related data sensitivities includes a design flaw which approaches something of a bad "Washington bureaucracy" joke: the challenge of cutting off access to sensitive data from foreign adversaries triggers CFIUS's policy realm and authority initially but ultimately implicates the functional role of the Federal Trade Commission ("FTC"). CFIUS scrutiny applies only to transactions where the foreign entity seeks to acquire some form of ownership interest – but sales of goods and information (as opposed to equity) would fall outside the statute. And even if a covered transaction triggers a CFIUS review, most of the work to counter the national security risk occurs on the front-end only, that is, review of the proposed foreign investment transaction itself. Even if this review results in the imposition of ongoing conditions through a "mitigation agreement"[55] (which is relatively rare), the Committee and its constituent agencies historically lacked staff and funding to carry out its functions, though hopefully this will change in the future.[56] Therefore, as more resources accrue to the Committee, it must develop the expertise and capacity to closely monitor and regulate data practices, assuming that such practices fall within its purview. Separately, the FTC *does* have a

53. 50 U.S.C. § 4565 (a)(4)(D)(i)(I-III).
54. *See* 31 C.F.R. § 800.241 (2022).
55. 31 C.F.R. §§ 800, 802 (2022).
56. U.S. GOV'T ACCOUNTABILITY OFF., GAO-18-249, TREASURY SHOULD COORDINATE ASSESSMENTS OF RESOURCES NEEDED TO ADDRESS INCREASED WORKLOAD (2008).

long history of regulating various trade practices, but the FTC has no apparent relationship with CFIUS and disclaims "national security" jurisdiction.[57]

The FTC's isolation from national security matters stems from its status as an independent government agency designed to support and foster commercial activity and to protect U.S. consumers. This extends, at least in part, to consumer protection with respect to their data.

The FTC's regulatory scope with respect to data trade and privacy also highlights a difference in data privacy values and theory between the United States and the EU. Already in 1995, the EU passed strict federal data privacy legislation, while the United States has taken a polar opposite "laissez-faire" approach,[58] declining to pass data privacy legislation except to account for certain sector-specific data sensitivities.[59] As a result, the general U.S. data privacy framework turns on pre-existing law such as the Electronic Privacy Act of 1986 ("ECPA"), which is lenient with respect to modern data transaction practices.[60] In this semi-vacuum, the FTC assumed the role of data privacy watchdog, and penalizing "unfair" or "deceptive" trade practices involving data under its foundational

57. Letter from Edith Ramirez, Chairwoman of the Fed. Trade Comm'n, to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality, European Commission (Feb. 23, 2016) (on file with Fed. Trade Comm'n).

58. *See, e.g.,* Robin Kurzer, *The United States Finally Starts to Talk About Data Privacy Legislation*, MARTECH (Aug. 10, 2018, 10:11 AM), https://perma.cc/KJS9-VZKX (quoting Neil Lustig, CEO of the marketing automation company Sailthru: "[The EU] government is more involved and has a more paternal approach to its citizens and their protections . . . In the US it's more of a laissez-faire capitalism approach that assumes that the market will ultimately solve these problems.").

59. While there is no generalized U.S. federal data privacy law equivalent to the EU's GDPR, Congress has passed federal data privacy regimes for certain sectors, *e.g.*, COPPA forbids data collection against minors, HIPAA restricts collection of medical information, etc.

60. ECPA contains two key statutory schemes governing data law: (A) the Stored Communications Act (the "SCA" – 18 U.S.C. § 2701 *et seq.*) and (B) the Wiretap Act (18 U.S.C. § 2511). These provisions apply to both government wiretapping as well as private data collection. The SCA bars companies holding electronic communications from circulating those communications unless the company has been so authorized. 18 U.S.C. § 2702(a). However, companies are free to look at content data on their own servers. 18 U.S.C. § 2701(c)(1). They are further free to circulate the content of communications (A) to "an addressee or intended recipient" of communications, or (B) "with the lawful consent" of the originator. 18 U.S.C. § 2702(b)(1-3). Not only do the restrictions of the SCA expressly apply only to content data, (18 U.S.C. § 2711(1)) but the SCA affirmatively establishes the prerogative of the company holding such non-content "records" to circulate this "to any person other than a government entity." *See* 18 U.S.C. § 2702(c)(6), § 2703(c). The Wiretap Act closely resembles the SCA, except that it addresses the collection (wiretapping) of information. Violations occur when any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). With respect to content data, the Wiretap Act forbids parties from divulging such data to third parties other than the addressee or intended recipient of a communication. 18 U.S.C. § 2511(3)(a). However, like the SCA, the Wiretap Act provides a broad exception for the "consent" of the originator, through which collection and transmission of content data to third parties is allowed. 18 U.S.C. § 2511(3)(b)(ii). Thus, the entire matter of data privacy and ECPA—the SCA and the Wiretap Act—is relatively narrow in practice: companies, including independent data brokers (whose entire business relies on the capacity to gather information) vacuum "non-content" data and build profiles of internet users even without needing access to content data. But of course, content data may be collected and disseminated as well, under both the SCA and the Wiretap Act's "consent" exceptions.

statute, the FTC Act of 1914. The FTC's data watchdog activities, guided by its consumer protection mandate, include (A) enforcing data security standards (to protect consumers from harm through data breaches) and (B) ensuring that companies do not breach their own representations or Terms of Service (TOS) agreements with consumers.

With respect to data security actions, the FTC recognized at the outset that establishing a technology-specific rule regime would be untenable because such rules would soon be rendered defunct by progress.[61] At the same time, more generalized rules about data security (less contingent on technology) would be impracticably vague.[62]

Anticipating this regulatory challenge, the FTC has instead constructed its framework for inadequate ("unfair") data security regimes through agency adjudication. Under the *Chenery* doctrine, government agencies have the option of conferring notice to the private sector by constructing a "common law"-type framework with individual adjudications:[63] hence, theoretically, after a certain number of FTC orders penalizing "unfair" cybersecurity regimes, these cases cumulatively establish parameters for cybersecurity protection requirements without rule-making. Cases of blatantly insufficient cybersecurity do not pose difficulties for the FTC.[64] More borderline cases, where "unfairness" must be established against a backdrop of shifting industry practices and other factors, have proven problematic for the FTC.[65]

In contrast to the data security "unfairness" determinations, the FTC's role with respect to data *privacy* (and trade) appears more stable because such scrutiny turns on the alignment between the representations of companies and their data conduct in practice – a stable target which, unlike data security standards, does not comparably shift with technological progress.

However, at the same time, the FTC has affirmatively disavowed "national security" related jurisdiction – for example, a public February 23, 2016, letter from FTC Chairwoman Edith Ramirez (published on the FTC website) states explicitly in a "Background" description of the FTC that "The FTC does not have jurisdiction over . . . national security matters."[66]

This appears to yield an awkward division of labor. As discussed briefly above, CFIUS screens foreign investments in U.S. companies which could give rise to

61. *See Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, 129 HARV. L. REV. 1120 (2019).

62. *Id.*

63. *See* SEC v. Chenery Corp., 332 U.S. 194 (1947) ("Chenery II"); *see also* Justin Hurwitz, Data Security and the FTC's UnCommon Law, 101 Iowa L. Rev. 955 (2016) ("[I]n *Chenery II* the Supreme Court gave agencies broad latitude in deciding whether to formulate rules through legislation-like rulemaking processes or to take a more standards-like approach to developing legal norms through common-law-like adjudicative processes.").

64. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 242 (3d Cir. 2015).

65. *See*, *e.g.*, Kirk Nahra, *Takeaways From the 11th Circuit FTC v. LabMD Decision*, IAPP (June 7, 2018), https://perma.cc/NH5M-X7WZ.

66. *See* Ramirez, *supra* note 57.

access to data sensitive on national security grounds. However, because this CFIUS scrutiny almost always applies at the investment stage only (except in the case of rare CFIUS mitigation agreements), CFIUS has limited involvement in functional data access and circulation.

The awkwardness of the relative responsibilities of CFIUS and the FTC is being noticed. Recent *Lawfare* reporting has highlighted this misalignment: in one of the CFIUS authority-based actions which drew universal praise, CFIUS forced a Chinese company to divest its ninety-eight percent holding in the LGBTQ dating app Grindr, which collects highly sensitive personal information, including the HIV status of its users.[67] But does this address the national security data threat if Chinese parties can simply make an agreement with Grindr or with a data broker to purchase the data without making an investment in the company? Kamran Kara-Pabani and Justin Sherman, writing in *Lawfare*, properly wonder:

> . . . a recent Norwegian government report on Grindr found that the application is sharing data with a range of third parties including data brokers—meaning data on the application's users is traveling far beyond the bounds of just that company. This all raises the question: Is forcing the sale of a sensitive-data-holding company from a Chinese firm enough to mitigate national security risks when the data can still end up in that Chinese firm's, or the Chinese government's, hands? [68]

Accordingly, Michael Kans reports in *Lawfare* that the FTC is also under-equipped to fill such a data practice scrutiny role:

> One must also consider the resource constraints of the agency that would presumably police the compliance of covered entities. The resource and staffing limitations of the FTC have been noted even if the agency received a $10 million bump for fiscal 2021. The FTC is unlikely to be able to thoroughly regulate the data brokering world based on its current funding, especially since it would be tasked with regulating the privacy and data protection practices of many more entities.[69]

In sum, CFIUS holds the policy role of guarding U.S. data from adversarial foreign interests by screening for ***access*** through foreign investments, while the FTC polices the functional ***circulation*** of data and disclaims "national security" jurisdiction (and does not possess the resources to fully assume such a role in any case). A recent Biden administration Executive Order on Cybersecurity referenced the FTC's role with respect to enforcing private sector data security

67. Kamran Kara-Pabani & Justin Sherman, *How a Norwegian Government Report Shows the Limits of CFIUS Data Reviews*, LAWFARE (May 3, 2021), https://perma.cc/56DU-FP62.

68. *Id.*

69. Michael Kans, *Data Brokers and National Security*, LAWFARE (Apr. 29, 2021), https://perma.cc/D4CK-5SNC.

practices (to protect consumers) but made no mention of any FTC role guarding against data practices and transactions giving rise to foreign adversarial access.[70]

In short, even if CFIUS successfully guards against foreign adversarial access via investment, non-investment related acquisitions of data (through multibillion-dollar data sale agreements) fall outside CFIUS's purview and appear to be more of an issue for the FTC. But the FTC is not legally or practically equipped (or willing) to widen the scope of its supervision of data circulation (and brokerage[71]) on national security grounds to supplement the CFIUS-FIRRMA framework. As we will examine below, the FTC's unclear authority in this area takes on added significance given the *TikTok v. Trump* decision's analysis of IEEPA.

D. Dames & Moore v. Regan

The governing constitutional decision for administrative national security law mechanisms such as IEEPA and CFIUS is *Dames & Moore v. Regan* (1983), featuring a fascinating and powerful opinion from Justice William Rehnquist, writing for a near-unanimous majority.[72]

Dames & Moore represented a dispute stemming from the settlement of the Iranian hostage crisis and the ouster of Shah Reza Pahlavi. Responding to the November 4, 1979, storming of the U.S. embassy and the hostage crisis, President Jimmy Carter declared an emergency, invoked IEEPA to freeze all Iranian assets in the United States, and directed the Treasury Department to carry out the order.[73] OFAC thereby issued a regulation declaring "any attachment, judgment, decree, lien, execution, garnishment, or other judicial process is null and void with respect to any property in which there existed an interest of Iran."[74]

On December 16, 1979, private construction and consulting firm Dames & Moore filed a $3.5 million suit against Iran and several Iranian institutions in federal court to collect on the firm's contract (pre-dating the Iranian Revolution) to conduct site studies for a proposed nuclear power plant in Iran. The District Court ordered an attachment against Iranian property.

Finally, on January 20, 1981, the hostages were released by Iran through a U.S.-Iran agreement which arranged (in part) the termination of all litigation between the government of each party and the nationals of the other, requiring that all such disputes be settled through arbitration.[75] Arbitration proceedings not settled in six months would be run through a Claims Tribunal.[76] Under these terms, the United States was obligated "to terminate all legal proceedings in United States courts involving claims of United States persons and institutions against Iran and its state enterprises, to nullify all attachments and judgments

70. Exec. Order No. 14,028, 86 Fed. Reg. 26,633 (May 17, 2021).
71. *See* Kans, *supra* note 69.
72. Dames & Moore v. Regan, 453 U.S. 654 (1983).
73. *Id.* at 662-63.
74. *Id.* at 663.
75. *Id.* at 665.
76. *Id.*

obtained therein, to prohibit all further litigation based on such claims, and to bring about the termination of such claims through binding arbitration."[77]

On January 19, 1981, President Carter acted to implement the terms of the Agreement in a series of Executive Orders.[78] On January 27, 1981, Dames & Moore moved for summary judgment in federal district court (contravening the settlement agreement between the U.S. and Iranian governments), and the court awarded them the amount claimed in their complaint plus interest. The firm attempted to execute the district court's judgment by obtaining writs of garnishment, leading to a planned sheriff's sale of Iranian property in the United States.[79]

However, on February 24, 1981, President Reagan issued further Executive Orders which "ratified" the Carter Orders.[80] Reagan "suspended" all "claims which may be presented to the [arbitration] Tribunal" and declared that such claims, including that of Dames & Moore, "shall have no legal effect in any action now pending in any court of the United States."[81] Hence, the Reagan Order, pursuant to the Carter Orders and underlying emergency declaration by Carter, worked through IEEPA and the NEA to prevent Dames & Moore from recovering its losses through judicial process. The litigation reached the Supreme Court, leaving the Court to assess the President's power to "nullify" the district court's attachments of the Iranian property and suspend the recovery claim.

In his majority opinion, Justice Rehnquist parsed IEEPA (and other administrative national security law mechanisms authorized through congressional action, such as CFIUS and ECRA) with reference to Justice Robert Jackson's famous concurring opinion in *Youngstown Sheet and Tube Co*. (collectively the Steel Seizure cases).[82] The Jackson executive power paradigm in *Youngstown* stipulated that executive power is at its zenith when the President acts with congressional support; when the Congress remains silent, executive power operates within a "zone of twilight"; and finally, executive power is at its "lowest ebb" when Congress opposes the President (and the disputed matter is domestic).[83]

Construing IEEPA with reference to the Jackson *Youngstown* paradigm in his majority opinion,[84] Justice Rehnquist reasoned that Congress's purpose in

77. *Id*.
78. *Id*. at 665-66.
79. *Id*. at 666.
80. *Id*.
81. *Id*.
82. *Id*. at 668-69 (citing Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring)).
83. *Id*. at 669 (citing *Youngstown*, 343 U.S. at 637-38 (Jackson, J., concurring)).
84. Justice Rehnquist did add a notable caveat, recognizing that classifying executive actions based on congressional support, silence, or opposition might not be cut-and-dried: "Although we have in the past found and do today find Justice Jackson's classification of executive actions into three general categories analytically useful, we should be mindful of Justice Holmes' admonition . . . that "[the] great ordinances of the Constitution do not establish and divide fields of black and white." Springer v. Philippine Islands, 277 U.S. 209, 209 (1928) (Holmes, J., dissenting)). Justice Jackson himself

passing IEEPA was "to put control of foreign assets in the hands of the President,"[85] triggering the congressional-support contingency of the Jackson *Youngstown* paradigm for domestic executive national security power. Accordingly, "[b]ecause the President's action in nullifying the attachments and ordering the transfer of the assets was taken pursuant to specific congressional authorization," it must be "**supported by the strongest presumption and the widest latitude of judicial interpretation, and the burden of persuasion would rest heavily upon any who might attack it**;" a finding against the government would mean that the "federal government as a whole lacked the power exercised by the President"[86] [emphasis added].

Notably, Rehnquist even went a step further. Not only did such administrative national security mechanisms enjoy maximal power because of congressional approval, but they even empowered the President to treat US-based foreign assets of adversarial countries as "bargaining chips"—"**such orders permit the President to maintain the foreign assets at his disposal for use in negotiating the resolution of a declared national emergency. The frozen assets serve as a 'bargaining chip' to be used by the President when dealing with a hostile country**"[87] [emphasis added].

The notion of the executive backed by Congress holding foreign assets of adversarial countries as "bargaining chips" aroused the concern of Justice Powell, who published a partial dissent emphasizing that such actions ought to trigger a government duty to pay just compensation to such foreign parties.[88]

Dames & Moore demonstrates that presidential decisions exercising IEEPA and other similar national security economic authorities enjoy broad judicial deference. Such deference extends, in the case of *Dames & Moore*, even to unwinding valid judicial decisions. But as we discuss below, the D.C. District Court in its *TikTok* decision deviated from this precedent in multiple ways. Does the *TikTok* decision mark a sea change from the executive-friendly precedent of *Dames & Moore*? We explain the significance of these potential changes below and in Part 4.

---

recognized that his three categories represented "a somewhat over-simplified grouping," and it is doubtless the case that executive action in any particular instance falls, not neatly in one of three pigeonholes, but rather at some point along a spectrum running from explicit congressional authorization to explicit congressional prohibition. Dames & Moore v. Regan, 453 U.S. 654, 669 (1983) (quoting *Youngstown*, 343 U.S. at 635 (Jackson, J., Concurring)). "This is particularly true as respects cases such as the one before us, involving responses to international crises the nature of which Congress can hardly have been expected to anticipate in any detail." *Id*. at 669.

85. *Dames & Moore*, 453 U.S. at 673 (quoting Propper v. Clark, 337 U.S. 472, 493 (1949)).

86. *Id*. at 674 (citing *Youngstown*, 343 U.S. at 636-37 (Jackson, J., concurring)).

87. *Dames & Moore*, 453 U.S. at 673.

88. *Id*. at 690-91 (Powell, J., dissenting).

PART 2: OVERVIEW OF THE FOREIGN BULK DATA COLLECTION PROBLEM BEFORE *TIKTOK V. TRUMP*

The *TikTok* case, and the "ban" which spawned it, does not arise in a vacuum. Broadly, the history of national security law is a saga of legal and bureaucratic adjustments responding to rapid technological and geopolitical developments. In this instance, these developments pertain to the explosion of personal data processing and transfers now underlying much of the global economy. The 9/11 attacks and the USA PATRIOT Act represented the transition from a Cold War posture to the War on Terrorism. Overlapping the latter part of this transition, foreign competitors—especially China—began targeting the United States economically through cyberspace.[89] While such foreign economic collection may be viewed as a mere cyber-based continuation of Cold War-era industrial espionage, cyber intrusions are distinct because of their scope (the amount of valuable data which can be extracted through one infiltration) as well as their potential severity (the level of damage to critical infrastructure possibly caused by remote actors).

Focused on terrorism in the post-9/11 period, the U.S. government and the West writ large were relatively slow to adapt to foreign economic collection in cyberspace.[90] The U.S. private sector also was not equipped to protect itself from the cyber espionage of adversarial nation states, and theoretically restricted from full cyber defensive measures under U.S. law. While the government previously protected the U.S. Defense Industrial Base ("DIB") from Soviet espionage during the Cold War, government protection of the DIB from prolific, computerized espionage was distinct, and challenging to coordinate.

As damage from foreign economic collection against the U.S. private sector escalated, companies independently fought back against hackers irrespective of legal constraints against such "hackbacks," otherwise known as "active defense." With the passage of the Cybersecurity Information Sharing Act (2015), the U.S. legal framework and government bureaucracy began enabling and facilitating cyber threat information sharing between the private sector and the government. Despite these and other improvements (such as the CISA Agency Act of 2018) industry still loses hundreds of billions of dollars annually to foreign economic collection in cyberspace.

The newest shift in this thread is subtle but significant. The private sector is on high alert to defend trade secrets and intellectual property, but the value of U.S. bulk data is growing dramatically, both for commercial and national security purposes. This is a novel phenomenon: it is a documented fact that during the Cold War, the U.S. Intelligence community collected eighty percent classified

89. *See generally* United States v. Huawei, No. 18-457, 2020 WL 1319126 (E.D.N.Y. Feb. 13, 2020), *superseding indictment*.

90. *See generally* Terence Check, *Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict: A NATO-Centric Approach,* 63 CLEV. ST. L. REV. 495, 497-502 (2015) (surveying Western and alternative characterizations of pressing cybersecurity issues at the time and analyzing official strategic documents that indicated that cyber threats ranked third in terms of priority). Needless to say, times have changed.

information and only twenty percent open-source information (for example *Pravda*).[91] At home, the U.S. IC focused centrally on protecting specialized classified technology relating to the DIB and expert individuals connected with the DIB. Likewise, the mid-twentieth century private sector—for example, the music industry—gathered as much information as possible about consumer behavior, but without computer technology there were practical limitations on how much individual or group consumer habits could be tracked and exploited to commercial ends. As noted above, the past non-value of ordinary communications data was even reflected directly in the text of IEEPA.[92]

However, with the rise of big data, these trends have been reversed on all three counts. First, intelligence operators around the world collect ordinary data and OSINT (inverting the old Cold War 80-20 ratio[93]) in bulk and use algorithms to cull such data. Second, the modern private sector has the technical capacity to mass-collect and synthesize information about consumer behavior (and every consumer individually), and to lucratively exploit this information from many different angles. Third, ordinary communications (for example, social media activity) now, clearly, have significant economic value.[94] Despite their inherent value, the fast-moving world of information technology makes it difficult for the government to quickly and effectively respond to potentially problematic data exports.

At this juncture, it is worth briefly detouring slightly to examine a case study that demonstrates these trends in practice, through the lens of biometric data. The reasons for this focus will become apparent to the reader – in a nutshell, biometric data is unique to an individual and is unchangeable.[95] Once obtained, the possessor of that data can share that data across platforms and spaces. There are good reasons for this capability. Biometrics enable the rapid identification and have assisted law enforcement agencies in solving crimes for more than a century.[96] In response to the 9/11 terror attacks and the rampages of Raphael Resendez-Ramirez, "the Railroad Killer," the federal government developed large-scale biometric databases like the FBI's Next Generation Identification System and the Department of Homeland Security's Automated Biometric Identification System.[97]

---

91. MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 104 (2009).

92. *See* 50 U.S.C. § 1702(b).

93. LOWENTHAL, *supra* note 91 at 104.

94. *See, e.g.*, *Win a Tesla Model S in Saweetie's Best Friend Giveaway,* BASS CAMP (2021), https://perma.cc/49XW-L7JH (asking for email addresses in exchange for two Tesla luxury cars).

95. U.S. DEP'T OF COM., NIST SPECIAL PUBL'N 800-12, AN INTRODUCTION TO INFORMATION SECURITY (2017), https://perma.cc/C9WK-BGAK.

96. *Biometrics,* DEP'T OF HOMELAND SEC. (July 13, 2020), https://perma.cc/QMJ2-VLF5.

97. *Id.* ("Despite multiple convictions for various offenses in the U.S. dating back to 1977 and seven apprehensions by Border Patrol, [Resendez-Ramirez] was routinely permitted to voluntarily return to Mexico. Border Patrol agents were unaware that the FBI and local authorities had outstanding arrest warrants for him for murder. Shortly after Resendez's return to Mexico, he illegally reentered the United States and committed four more murders before surrendering to law enforcement. This brought about a review of IDENT and calls for the integration of IDENT with the FBI's fingerprint database."); *see also*

Despite these instances of constructively using biometric data to support public safety, a growing number of privacy groups claim that biometric data poses severe risks to personal privacy.[98] Even so, the use of such technology has proliferated widely in the past few years.[99] Once the province of law enforcement agencies and science fiction, most Americans now have highly sophisticated biometric sensors incorporated into their mobile phones.[100] According to the University of Texas at Austin's Center for Identity, the ubiquity of personal smart devices has led to a growing number of potential applications for biometric technology to identify users and authenticate a vast number of transactions across multiple sectors.[101] Such sectors include software and arts/recreation, with the extreme popularity of sophisticated mobile apps offering face filters as a prominent example.[102]

Unsurprisingly then, given the user demand for innovative filters, a mobile application called FaceApp went viral in the summer of 2019. Hundreds of millions of smartphone users the world over downloaded the niche app, which took facial photographs of the users and convincingly rendered age-progression portraits in a matter of seconds, all for free.[103] Social media amplified the reach of FaceApp online, proliferating widely within days. Then, eagle-eyed observers noticed that FaceApp originated in Russia, a perennial counterintelligence, security, and economic threat to the United States and its allies.[104] Responding to the rising panic, media outlets and FaceApp leadership addressed the growing privacy and security concerns: "the darkest fears of a Russian connection, researchers and technical experts said Thursday, appeared to have been overblown."[105] According to these reports and FaceApp's statement, the processing of users'

---

8 U.S.C. § 1365b(a) ("Consistent with the report of the National Commission on Terrorist Attacks Upon the United States, Congress finds that completing a biometric entry and exit data system as expeditiously as possible is an essential investment in efforts to protect the United States by preventing the entry of terrorists.").

98. U.S. DEP'T OF COM, *supra* note 95, at 62-63.

99. Rachel German & K. Suzanne Barber, *Current Biometric Adoptions and Trends,* UNIV. OF TEX. AT AUSTIN CTR. FOR IDENTITY, https://perma.cc/V6HH-DGFB ("Governmental use of biometric to identify citizens for various purposes is increasing alongside consumer trends. According to ABI Research, the biometrics market will reach $30 billion by 2021.").

100. *Id.*

101. *Id.* at 11 ("The previous four years (2012-2016) have seen a rapid increase in the rollout of new biometric technologies in multiple market sectors, with finance and information technology leading the charge.").

102. James Le, *Snapchat's Filters: How Computer Vision Recognizes Your Face,* MEDIUM (Jan. 28, 2018), https://perma.cc/AJF2-7P8D; Alyson Shontell, *Snapchat Buys Looksery, a 2-Year-Old Startup That Lets You Photoshop Your face While You Video Chat*, BUS. INSIDER (Sep. 15, 2015, 3:36 PM), https://perma.cc/T7XW-3P6R.

103. John Koetsier*, Viral FaceApp Now Owns Access to More Than 150 Million People's Faces,* FORBES (July 17, 2019, 12:38 PM), https://perma.cc/F7QK-MYEA.

104. Hannah Denham & Drew Harwell, *Panic over Russian Company's FaceApp Is a Sign of New Distrust of the Internet*, WASH. POST (July 18, 2019, 6:46 PM), https://perma.cc/K8VS-TVRX**;** *Worldwide Threat Assessment of the US Intelligence Community*, 116th Cong. 5 (2019) (statement of Daniel R. Coates, Director of National Intelligence).

105. Denham et al., *supra* note 104; Natasha Lomas, *FaceApp Privacy Concerns,* TECHCRUNCH (July 17, 2019, 10:57 AM), https://perma.cc/K4UM-DCLA.

facial recognition and other data took place in the cloud on infrastructure outside of Russia.[106] Furthermore, FaceApp claimed that it transferred "no data" to Russia, even though its R&D facilities resided there.[107] Even so, the phrasing of the Company's statement given to popular tech media outlet TechCrunch left concerning wiggle room. For example, the company stated that "We might store an uploaded photo in the cloud" and "Most images are deleted from its servers within 48 hours."[108] Despite company claims made in July 2019 that it does not sell facial data or transfer data to Russia, its current Terms of Use allow for both.[109] After the initial fervor died down, the Federal Bureau of Investigation later confirmed that despite prior claims of privacy and data protection, FaceApp remained a "counterintelligence threat" due to its connections to Russia.[110] In response to the FBI's findings, CompTIA security expert Ian Thornton-Trump admitted that even though the specific risk to ordinary Americans remains low, there remain "national security considerations with any data being held in an adversarial or politically non-aligned country," pointing to the lack of any controls on commercial enterprises and their ability to support intelligence gathering and espionage for nation-state rivals.[111]

The FaceApp case shows that a software company with ties to a serious geopolitical competitor of the United States can easily and cheaply acquire unique and sensitive data on American citizens within a matter of days for virtually unregulated use, use which could include access by foreign security services.[112] The nuanced and quickly-developing information regarding FaceApp could have confused even a well-informed and savvy consumer, even though large technology platforms like Apple and Google often make no effort to hide the foreign provenance of a particular product. Downloading and using these apps frequently involves little to no friction for the user.[113] Managing access and reuse of personal data becomes difficult once consumers entrust their data to technology companies: it can be difficult to unwind these transfers once consumers provide their information and invite these applications onto their devices.[114] These dynamics

106. Lomas, *supra* note 105.

107. *Id.*

108. *Id.* [emphasis added].

109. *FaceApp Terms of Use Agreement*, FACEAPP (Dec. 3, 2019), https://perma.cc/AS4P-5VAG ("You grant FaceApp a nonexclusive, royalty-free, worldwide, fully paid license to use, reproduce, modify, adapt, create derivative works from, distribute, perform and display your User Content during the term of this Agreement solely to provide you with the Services . . . By accessing or using our Services, you acknowledge and, as applicable, consent to the processing, transfer and storage of information about you in and to the United States and other countries.").

110. Kate O'Flaherty, *The FBI Investigated FaceApp. Here's What It Found,* FORBES (Dec. 3, 2019, 6:31 AM), https://perma.cc/556V-SWGA; *see also FBI Says Russian FaceApp Is 'Potential Counterintelligence Threat','* REUTERS (Dec. 2, 2019, 4:33 PM), https://perma.cc/JH2R-UY8Z.

111. O'Flaherty, *supra* note 110.

112. REUTERS, *supra* note 110.

113. *Understanding Mobile Apps,* FED. TRADE COMM'N (May 2021), https://perma.cc/F5VS-V7LM.

114. Gabriel J.X. Dance, Michael LaForgia & Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://perma.cc/AG7J-LR9P ("[D]ocuments, as well as interviews with about 50 former employees of Facebook and its corporate

become particularly dangerous when coupled with "sticky" social media applications that provide countless hours of entertainment and other benefits to their users, and generating significant economic activity.

These dynamics have also been prominently reflected in the discourse surrounding two leading Chinese tech companies, Huawei and ZTE, which have played prominent roles in the history of foreign economic collection through cyberspace. The most recent U.S. superseding criminal indictment of Huawei alleges that the company has been prolifically engaged in stealing U.S. intellectual property, such as technology and trade secrets, for more than twenty years.[115]

In 2018, the U.S. Intelligence community warned *the public at large* (rather than merely the private sector) that Huawei and ZTE presented a threat not merely because of traditional cyber foreign economic collection of national security information but because of their wider, more general collection of quotidian U.S. person information on behalf of the Chinese Communist Party.[116] In the case of social media (distinct from device manufacturers like Huawei), these applications provide significant value to their users. And many users either do not know or do not care about the risks posed to their personal information by potential access by rival foreign powers through these applications. Seemingly, consumers will give continued assent to data processing in these circumstances, begrudgingly making more of their data available despite increasing general distrust of social media platforms: these platforms are simply too practical to quit.[117] Given these market forces, the complex threat environment, and the sensitive, unchangeable nature of biometric information in particular, should the United States government take steps to restrict cross-border sales or transfers of biometric data even if consumers otherwise provide their consent?

The collective trajectory of these developments points toward policy makers increasingly attempting to invoke national security-based economic regulatory authorities—IEEPA, CFIUS, and the Export Control Reform Act of 2018 ("ECRA")—to restrict foreign access to information which is increasingly distant from conventional "national security" information, that is, data stemming from conventional internet commerce and discourse. In other words, economic power under the aegis of national security—traditionally applied, for example sanctions against rogue regimes and dictatorships for terrorism, weapons proliferation,

---

partners, reveal that Facebook allowed certain companies access to data despite those protections. They also raise questions about whether Facebook ran afoul of a 2011 consent agreement with the Federal Trade Commission that barred the social network from sharing user data without explicit permission.").

115. United States v. Huawei, No. 18-457, 2020 WL 1319126, at *7-12 (E.D.N.Y. Feb. 13, 2020), *superseding indictment*.

116. Salinas, *supra* note 6.

117. Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns,* PEW RSCH. CTR. (Mar. 27, 2018), https://perma.cc/8BVL-H8LK ("The paradox is that people use social media platforms even as they express great concern about the privacy implications of doing so – and the social woes they encounter. The Center's most recent survey about social media found that 59% of users said it would not be difficult to give up these sites, yet the share saying these sites would be hard to give up grew 12 percentage points from early 2014.").

slavery, corruption, war crimes and genocides[118]—will be turned, for legitimate reasons, toward what may appear, incorrectly, as relatively marginal ends.

Accordingly, in 2019-20, the Trump administration took measures to stem the flow of U.S. data to China by targeting TikTok, a social media and User-Generated Content ("UGC") platform owned by the Chinese tech company ByteDance. In November 2019, Reuters announced that CFIUS—empowered to unwind foreign investments in U.S. companies—had opened an investigation into ByteDance's prior purchase of TikTok in 2017.[119] Then, in July 2020, President Trump invoked IEEPA to respond to "extraordinary and unusual threats"—that TikTok posed a risk to the national security of the United States to effectively ban all TikTok transactions in the United States.[120] The U.S. government's findings on national security risks posed by TikTok focused on two concerns relating to the flow of data and information in and out of the United States.[121] TikTok could provide a channel for the exposure of millions of Americans, particularly teenagers and young adults, to propaganda from the Chinese Communist Party.[122] Of greater relevance to this article, EO 13942 also explained that the automated collection of personal information, including internet browsing patterns, could enable the Chinese government to "access … Americans' personal and proprietary information— potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[123]

Based on this assessment, the executive branch took two sets of actions. The first prohibited "transactions" under IEEPA, which effectively would result in a ban on downloads and updates of the TikTok app within the United States.[124] The second set of actions focused on the use of the foreign investment review process managed by CFIUS to ensure that Bytedance, another Chinese tech company with close ties to the Chinese Communist Party,[125] would divest itself of its ownership interest in TikTok, allowing some other company that did not pose the same national security concerns to purchase Bytedance's stake.[126]

---

118. *See generally* Elena Chachko, *Administrative National Security*, 108 GEO. L.J. 1063 (2019).

119. ByteDance had acquired TikTok's predecessor, Musical.ly, which had then become TikTok after it was merged with another app. *See* Greg Roumeliotis, Yingzhi Yang, Echo Wang & Alexandra Alper, *Exclusive: U.S. Opens National Security Investigation into TikTok – Sources*, REUTERS (Nov. 1, 2019), https://perma.cc/S6MV-3XQR.

120. Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020).

121. *Id.*

122. *Id.*

123. *Id.*

124. *See TikTok v. Trump*, 507 F. Supp. 3d 92, 96 (D.D.C. 2020). *See also* Identification of Prohibited Transactions to Implement Executive Order 13942 and Address the Threat Posed by TikTok and the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 60,061, 60,062 (Sept. 24, 2020).

125. *Id. at 3.*

126. *Id.* at 5. *See also* David E. Sanger, David McCabe & Erin Griffith, *Oracle Chosen as TikTok's Tech Partner, as Microsoft's Bid Is Rejected*, N.Y. TIMES (Sept. 14, 2020), https://perma.cc/756E-5998.

These dual maneuvers—the CFIUS investigation and the IEEPA orders—set the stage for a notional application of U.S. administrative national security frameworks to stop foreign data transactions and data flow to adversarial nations in spite of the enormous level of commerce generated from such activity. In this next section, we examine some of these frameworks and their applicability to the foreign data export issues discussed in the TikTok case.

PART 3: *TIKTOK V. TRUMP*: APPLYING IEEPA AND CFIUS TO FOREIGN ADVERSARIAL DATA ACCESS

After IEEPA authority was invoked against TikTok in August 2020, TikTok filed a suit with the D.C. District Court requesting an emergency injunction. Specifically, TikTok alleged that the IEEPA order had violated the First Amendment, the Fifth Amendment (due process and the takings clause), and the text of the IEEPA statute.[127]

Historically, challenges to IEEPA orders have been generally unsuccessful. This is unsurprising given the latitude conferred in *Dames & Moore*, construing IEEPA as reflecting maximum governmental authority (both the powers of Congress and the executive)—the highest possible legal power available under the constitutional system.[128]

However, irrespective of the latitude outlined by *Dames & Moore*, the IEEPA statute does state:

> [t]he authority granted to the President . . . does not include the authority to regulate or prohibit, directly or indirectly:
>
> any . . . personal communication, which does not involve a transfer of anything of value;
>
> [or]
>
> the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, . . . artworks, and news wire feeds.[129]

In response to these conditions, despite overwhelming executive power authority supporting IEEPA, the D.C. District Court granted the emergency injunction.[130] Reflecting the statutory language, the Court held that TikTok activity fell within the IEEPA exception for "personal communication[s] which do[] not involve a transfer of anything of value."[131] The Court also held that TikTok activity fell within the IEEPA exception barring restrictions on the importation or

127. TikTok v. Trump, 507 F. Supp. 3d at 100.
128. *See generally* CASEY, *supra* note 16.
129. 50 U.S.C. § 1702(b).
130. *See* TikTok v. Trump, 490 F. Supp. 3d 73 (D.D.C. 2020).
131. 50 U.S.C. § 1702(b)(1).

exportation of "informational materials" such as "publications, films . . . photographs, . . . artworks, . . . and news wire feeds."[132]

Neither of the legs of the Court's decision granting the injunction is fully comfortable. First, the holding that TikTok activity entails "personal communications which do not involve a transfer of anything of value" runs against the realities of the modern data economy, and uncannily echoes Leonard Santos's 1977 warning that such economic activity framed as "communications" would incidentally fall outside the scope of the IEEPA statute as drafted—for example, a contract mailed in an envelope.[133] Second, while the longstanding bipartisan anti-totalitarian policy of encouraging free international flow of ideas and information had (and has) obvious merit, the pre-IT era common understanding of "photograph," "film," "artwork" and "news wire feed" certainly did not include or reflect the idea that such items entailed instantaneous bulk collection and transmission of the data of those who produced and accessed them.

A. Recognition of TikTok's bulk collection of U.S. person data

While reasonable minds may differ as to optimal legal and policy answers for the challenges posed by foreign adversarial collection of U.S. person data and companies such as TikTok, reasonable minds may *not* differ as to the general rapid progress of data technology—and that this, in the hands of U.S. adversaries, represents at minimum a significant potential national security threat and likely an actual threat.

TikTok's data collection practices aroused the concerns of the FTC even before the Trump administration confronted the company on national security grounds: On February 27, 2019, the FTC fined ByteDance, the parent company of TikTok, $5.7 million for collecting the data of minors under age 13, a violation of the Children's Online Privacy Protection Act ("COPPA"), the largest ever COPPA-related fine.[134] While some readers may regard the FTC's $5.7 million fine as negligible given TikTok's $400 billion[135] valuation, FTC data privacy and security fines are regarded as inflicting reputational damage[136] so that the scope of an FTC sanction is not reflected by its direct sum.

A fine for collecting information on children might be regarded as a TikTok technical oversight rather than as a reflection of TikTok's strategy, intentions, and links to China. However, the scope of TikTok's data collection and the national security threat this poses is difficult to overlook.

---

132. 50 U.S.C. § 1702(b)(3).

133. *Id.*

134. Lesley Fair, *Largest FTC COPPA Settlement Requires Musical.ly To Change Its Tune*, FED. TRADE COMM'N (Feb. 27, 2019) https://perma.cc/4GKZ-XGKS.

135. Venus Feng & Zheping Huang, *TikTok Founder's $60 Billion Fortune Places Him Among the World's Richest People*, BLOOMBERG WEALTH (Apr. 13, 2021, 6:03 P.M.), https://perma.cc/A6XM-CT7Z.

136. *See* Dune Lawrence, *A Leak Wounded This Company. Fighting the Feds Finished It Off*, BLOOMBERG (Apr. 25, 2016), https://perma.cc/9Z3E-26TJ.

Indeed, despite striking down the IEEPA Order, the D.C. District Court widely recognized the breadth of TikTok's data collection practices under TikTok's own Terms of Service, which confirms bulk collection of the following types of data, which, as we foreshadowed above in Part 2, includes biometric data:

1. Registration information, such as age, username and password, language and email or phone number
2. Profile information, such as name, social media account information, and profile image
3. User-generated content, including comments, photographs, videos, and virtual item videos that you choose to upload or broadcast on the platform
4. Payment information, such as PayPal or other third-party payment information (where required for the purpose of payment)
5. Phone and social network contacts (names and profiles)
6. Opt-in choices and communications preferences
7. Information in correspondence users send to TikTok
8. Information sent by users through surveys or participation in challenges, sweepstakes, or contests such as gender, age, likeness, and preferences.[137]

Furthermore, "TikTok's core value to users lies in its ability to transmit data like 'text, images, video and audio,' all of which constitute 'bulk data' that . . . might be used by China 'to train algorithms for facial and voice recognition'"[138] (and while the D.C. District Court used the word "might," the prediction soon came true[139]). The court also pointed out express confirmation that such data was being used for intelligence purposes: "TikTok's Terms of Service and Privacy Policy . . . allow TikTok to collect and share a user's information with the . . . People's Republic of China to respond to 'government inquiries.'"[140] In addition, the court accepted a Commerce Department Memorandum exploring the specific uses to which TikTok-derived data is being employed:

> The Commerce Memorandum found that the PRC is "building massive databases of Americans' personal information" to help the "Chinese government to further its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment." It also concluded that the CCP will exploit "close ties" with ByteDance to further its foreign policy agenda. ByteDance is headquartered in Beijing and remains

137. TikTok v. Trump, 507 F. Supp. 3d 92, 99 (D.D.C. 2020).

138. *Id.*

139. Sean Keane, *TikTok is Letting Itself Collect Your Biometric Data*, CNET (June 4, 2021, 7:59 A. M.), https://perma.cc/H33L-M6HK.

140. TikTok v. Trump, 507 F. Supp. 3d at 99.

> subject to the PRC's National Intelligence Law, which "permits Chinese intelligence institutions" to "take control of" any China-based firm's "facilities" and "communications equipment." ByteDance has already signed a cooperation agreement with a PRC security agency, closed one of its media platforms in response to CCP demands, and (as of August 2020) placed over 130 CCP committee members in management positions throughout the company. And because "ByteDance is subject to PRC jurisdiction, [and] PRC laws can compel cooperation from ByteDance, regardless of whether ByteDance's subsidiaries are located outside the territory of the PRC," the data held by ByteDance's subsidiary companies may also be extracted by the PRC.[141] [citations omitted]

In other words, the court recognized ironclad evidence of (A) mass-collection of U.S. person data by TikTok and (B) direct contractual links between this data and the Chinese government.

B. The CFIUS and IEEPA Orders leading up to TikTok v. Trump

On November 1, 2019, eight months after the FTC COPPA fine against TikTok, Reuters reported that CFIUS was investigating the November 9, 2017, acquisition of TikTok by Bytedance.[142] At the time, TikTok had become the top downloaded app in the world, with two billion downloads worldwide and 130 million U.S. downloads. The November 9 transaction had not been submitted for approval to CFIUS despite TikTok's prolific business within the United States and mass collection of personal identifiable information on U.S. users.

As reviewed above, CFIUS may review any foreign investment in a U.S. company, including retroactively back to 1988. And, under CFIUS authority, the President may "take such action . . . as consider[ed] appropriate to suspend or prohibit any covered transaction that threatens to impair the national security of the United States," including the power to instruct the Attorney General to move for divestment (of assets from foreign parties) in U.S. district courts.[143]

With CFIUS proceedings against TikTok ongoing, the Trump administration engaged IEEPA authority against TikTok as well, overlapping the CFIUS investigation. As noted above, to invoke IEEPA, the President must declare a national emergency under the National Emergencies Act and then issue the IEEPA order pursuant to that declaration (with the option of working through an existing declaration that remains active). IEEPA thereby confers the power to "prevent or prohibit any . . . transactions involving . . . any property in which any foreign country of a national thereof has any interest by any person."[144]

President Trump declared a pertinent national emergency on May 15, 2019 with Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain." Executive Order 13873 contended:

---

141. *Id.* at 98-99.
142. *See* Roumeliotis et al., *supra* note 119.
143. 50 U.S.C. § 4565(d)(3); 50 U.S.C. app. § 2170.
144. 50 U.S.C. § 1702(a)(1)(B)).

> The unrestricted acquisition or use in the U.S. of information and communications technology or services designed, developed, manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects.[145]

Executive Order 13873 therefore prohibits transactions of this kind, based on a finding by the Commerce Secretary (in consultation with other officials) that:

1. The technology or service in question is associated with an entity subject to the jurisdiction or direction of a foreign adversary; and
2. The situation poses an undue risk of (a) sabotage of information and communication services in the U.S., (b) catastrophic effects on U.S. critical infrastructure or the digital economy or (c) **otherwise poses an unacceptable risk to U.S. national security.**[146] [emphasis added]

On August 6, 2020, acting through the emergency declaration of Executive Order 13873, Trump issued Executive Orders 13942 and 13943, thereby classifying TikTok and also WeChat—a Chinese communications and social media app—as "pos[ing] an unacceptable risk to U.S. national security," and invoked IEEPA to prohibit (ban) all TikTok and WeChat transactions as of mid-September.

The TikTok Executive Order (August 6, 2020)[147] linked the TikTok national security threat to the underlying national emergency,[148] alleging that such a social media video platform, if owned by Chinese interests, gives rise to security liabilities because (1) TikTok aggregates the U.S. user data which is accessible to the

145. Exec. Order No. 13,873, 84 Fed. Reg. 22,689 (May 15, 2019).

146. *Id.*

147. On August 14, 2020, President Trump additionally issued a CFIUS-based Divestment Order, announcing a finding that "credible evidence leads me to believe that ByteDance Ltd. . . . might take action that threatens to impair the national security of the United States." (*See generally* 50 U.S.C. § 4565(d)(4) (50 U.S.C. app. § 2170 (1988)).) Trump's order stated that his review and finding, prohibiting the ByteDance purchase of TikTok, had weighed the presidential finding factors as directed under the CFIUS framework, 50 U.S.C. § 4565(f). Trump's CFIUS-based Divestment Order stated:

> The transaction resulting in the acquisition by ByteDance of [TikTok], to the extent that [TikTok] or any of its assets is used in furtherance or support of, or relating to, [TikTok's] activities in interstate commerce in the United States ("[TikTok] in the United States"), is hereby prohibited, and ownership by ByteDance of any interest in [TikTok] in the United States, whether effected directly or indirectly through ByteDance, or through ByteDance's subsidiaries, affiliates, or Chinese shareholders, is also prohibited. Order Regarding the Acquisition of Musical.ly by ByteDance Ltd., (Aug. 14, 2020), https://perma.cc/S5AY-HGZS.

148. Executive Order No. 13,873 (May 15, 2019).

Chinese Communist Party, (2) TikTok censors and controls information, and (3) the Chinese Communist Party can use TikTok to circulate disinformation.[149]

C. TikTok v. Trump

IEEPA contains no provisions channeling legal review, except for a condition requiring that classified information, if submitted, must be reviewed *ex parte* and *in camera*.[150] Therefore, with no standard of review specified in the IEEPA statute, the Administrative Procedure Act ("APA") governs such reviews, applying a default rule that IEEPA orders may be reversed if recognized as "arbitrary, capricious, an abuse of discretion, or not otherwise not in accordance with the law."[151]

Courts adjudicating IEEPA procedural due process challenges apply the administrative law balancing test from *Matthews v. Eldridge*.[152] Under the *Eldridge* test, courts must weigh (1) the regulated party's property interest, (2) the risk of erroneous deprivation through the administrative process applied, and the value of additional safeguards, and (3) the government interest in maintaining its procedures, and burden of imposing additional procedural protections.[153] However, partially under *Dames & Moore*, the powers available under IEEPA are afforded such weight that even when courts have found that a regulated party has a strong property interest, this is outweighed by the overwhelming governmental interest.[154]

TikTok's request for an emergency injunction triggered a substantive ruling because such injunctions turn on a court's evaluation of the likelihood that the moving party's lawsuit will succeed. Generally, to secure an emergency injunction, a plaintiff seeking relief must demonstrate (1) a likelihood that the case will succeed on the merits, (2) irreparable harm if the injunction is not awarded, (3) that the balance of equities favors relief, and (4) that the injunction is in the public interest. In this case, the D.C. District Court's main inquiry in applying the test was prong 1, the likelihood of TikTok's success.[155]

The D.C. District Court accepted TikTok's argument that the IEEPA statutory text forecloses the application of such authorities to user data and held that the TikTok ban therefore "likely exceeded IEEPA's express limitations as part of an agency action that was arbitrary and capricious."[156] The Court ultimately issued two linked rulings: On September 27, 2020, the court granted a preliminary

149. Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020), *revoked by* Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021).

150. 50 U.S.C. § 1702(c).

151. *See* Chachko, *supra* note 118, at 1100 (citing Al Haramain Islamic Found., Inc., 686 F.3d 965, 976 ("The judicial review provisions of the Administrative Procedure Act . . . govern challenges to OFAC's designation decisions.") (citing also Alaska Dep't of Env't Conservation v. EPA, 540 U.S. 461, 496–97, 496 n.18 (2004)); 5 U.S.C.§ 706(2)(A)(2012).

152. *See* Mathews v. Eldridge, 424 U.S. 319 (1976).

153. *Id.*

154. *See, e.g.*, Al Haramain Islamic Found. v. U.S. Dep't of Treasury, 686 F. 3d 965, 980 (9th Cir. 2012).

155. *See* TikTok v. Trump, 490 F. Supp. 3d 73, 80 (D.D.C. 2020).

156. *Id.*

injunction, finding a likelihood of success on the merits and suspending the government's proposed download ban just as it was about to take effect.[157] The court then maintained the injunction in a similar ruling on December 7.[158]

The D.C. District Court's *TikTok v. Trump* opinions have multiple layers that this article need not analyze, such as whether the ban involved indirect or direct regulation for the purposes of IEEPA.[159] As noted above, the Court granted an injunction on the IEEPA order by holding that (1) TikTok's data transmissions constituted "personal communications which do[] not involve anything of value" and (2) TikTok content amounted to protected "informational materials."

1. "Personal Communications which do[] not involve a transfer of anything of value"

The court held that the transactions between TikTok users and TikTok (as well as between the users themselves) constituted personal communications that were not a "thing of value," and therefore the President's IEEPA powers could not reach such transactions.[160] At the heart of the court's analysis, TikTok asserted, and the court accepted, that "a wide swath of TikTok videos, public comments . . . and private messages between friends about TikTok videos" are "personal communications with no economic value at all."[161]

The U.S. government maintained that communications on TikTok possessed economic value in some cases.[162] For example, a handful of young adults have generated millions of dollars in net worth from their TikTok content and their large followings, enabling them to sign lucrative sponsorship deals with reputable companies such as Sony, Revlon, and Burger King.[163] Ad campaigns on TikTok can cost companies thousands of dollars per day and can utilize popular influencers to amplify their messages because TikTok's young audience "need[s] to get inspired by people they admire to join your challenge."[164] Companies need only to "choose a few influencers popular in different demographic segments, and you'll nail it."[165] Though the court conceded that "some" of this content might have value, it asserts, without citing any evidence, that a significant proportion of TikTok content and engagement comprises "no economic value at all."[166]

157. TikTok v. Trump, 490 F. Supp. 3d 73 (D.D.C. 2020).

158. TikTok v. Trump, 590 F. Supp. 3d 92 (D.D.C. 2020).

159. *Id.* at 103-07.

160. *Id.* at 107-108. *See also* 50 U.S.C. § 1702(b)(2) ("The authority granted to the President . . . does not include the authority to regulate or prohibit, directly or indirectly": any . . . any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value.")

161. TikTok v. Trump, 590 F. Supp. 3d at 107.

162. *Id.*

163. Abram Brown, *TikTok's 7 Highest-Earning Stars: New Forbes List Led By Teen Queens Addison Rae And Charli D'Amelio*, Forbes (Aug. 6, 2020), https://perma.cc/77H4-PHMA.

164. *Id.*

165. *Id.*

166. *TikTok*, 507 F. Supp. 3d at 107.

But this is not the case. Unlike text messages or emails, which have little to no ability to promote brands or function as micro-targeted advertising, TikTok content has tremendous value, including monetary value. In the world of TikTok, users are the billboard, the agency that makes the ad, and the drivers on the highway. TikTok utilizes content sharing and the virality of such content to generate its revenue, involving users in sharing content or even creating their own content to promote particular brands or messages. For example, thirty-five percent of all TikTok users have themselves participated in a "hashtag challenge" whereby they create content (such as re-decorating a dorm) on TikTok that supports a company's advertising campaign (such as a grocery store chain).[167] This engagement makes users and their communications unlike phone customers having conversations through AT&T's network: instead, TikTok traffics in, promotes, and derives unique value from its users' personal communications. Even though the rate of the number of "valuable" messages should not matter for purposes of interpreting IEEPA (the platform either has personal communications of value or it does not; in other words, IEEPA contains no de minimis requirement), thirty-five percent of all users participating in this type of activity means that there are more than "some" communications that have value and certainly more than the de minimis amount that the court seems to suggest.[168]

The rise of non-fungible tokens (NFTs) demonstrates an additional problem with the court's analysis of the personal communications exception to IEEPA because NFTs conclusively show that these TikTok messages and videos have their own intrinsic value.

The ACLU, in opposing the U.S. government's attempted ban on TikTok in the court of public opinion, stated:

> . . .online communities created by TikTok and WeChat are important to their users. People derive joy from posting songs and videos, or de-stressing in these stressful times with games or images of cats sitting in boxes. Simply sending a ♡ emoji to a family member or friend is a meaningful personal communication. People also use the apps for political activism. Influencers like Jalaiah Harmon, James Jones, and Addison Rae have hundreds to millions of followers on TikTok — with all the fun, earnings, and political influence it can bring. "Favoriting" or "liking" a post can convey meaning. It can also be

167. Adelina Karpenkova, *How to Advertise on TikTok (And Should You?)*, JOINATIVE (Sep. 22, 2020), https://perma.cc/7J8W-BXGD ("Branded Hashtag Challenge is an exclusive TikTok feature. You can find branded hashtags on TikTok's Discovery page. If you click on a sponsored hashtag, you'll be taken to a TikTok page with a brand logo, link to the company website, challenge description, and a list of popular videos that use the hashtag. Hashtag challenges are viral campaigns that allow brands to enter TikTok and gain followers fast. For ecommerce brands willing to benefit with hashtag challenges, TikTok adds a shoppable component to the hashtag, called the Hashtag Challenge Plus. The feature is yet to be released officially, but it has already been tested by Kroger, an American retail company."). *See also* Garrett Sloane & Lindsay Rittenhouse, *A Leaked Pitch Deck Reveals How TikTok is Trying to Woo Brands*, ADAGE (Oct. 9, 2019), https://perma.cc/G28M-65VK.

168. *Contra* TikTok, 507 F. Supp. 3d at 107-08.

> financially important to the platform and to the businesses that advertise their goods and services based on that expressive information. . ..[169]

But the *TikTok v. Trump* decision cites no authority for the proposition that such lucrative advertising content should not constitute a "thing of value" for the purposes of Section 1702.

The music and recording industry, for example, broadly corroborates the substantial value of these types of cross-border data exchanges; it is routine for enormous sums to change hands in exchange for inducing spikes in views/play/social media activity, all with the purpose of promoting an artist or song on a professional content platform.[170]

However, in its December 7, 2020, decision, the court applied a far narrower reading of a "thing of value," namely that TikTok content could not form a "thing of value" because it does involve a "transfer of money (or other value) as a part of the personal communication itself. . ."[171]

Thus, ultimately, the D.C. District Court's rulings zoomed in on the language flagged by Santos: "'personal communication[s] which do [] not involve a transfer of anything of value.'"[172] The court expressed concern that if quotidian data (such as messages sent by TikTok users) was found to have "value," this "would write the personal-communications limitation out of the statute."[173]

2. "Informational Materials"

The prima facie analogy between TikTok app user activity and circulation of "informational materials" barred from restriction under IEEPA (1977) – e.g., "photographs," film," "artwork, and "news wire feed[s]" – is self-evident. But as noted above, the analogy is not straightforward because of dramatic distinctions between the pre-IT era "informational materials" and big data social networking. We explain the strained quality of this reasoning-by-analogy below.

While Supreme Court jurisprudence might have pointed the Government towards definitional arguments about "photographs," "film," "artwork," and "newswire feeds" in the pre-IT era versus 2022,[174] the Government essentially conceded that TikTok engagement entails transmission of "informational

---

169. Hina Shamsi, Jennifer Stisa Granick & Daniel Kahn Gillmor, *Don't Ban TikTok and WeChat*, ACLU (Aug. 14, 2020), https://perma.cc/4ZDZ-4HFK.

170. *See generally* KERRY SEGRAVE, PAYOLA IN THE MUSIC INDUSTRY: A HISTORY, 1880-1991 (1994) (demonstrating historical practice of the music industry's use of radio to generate hits by negotiating a certain number of plays of a particular song); *Office of Justice Programs Summary*, U.S. DEP'T OF JUSTICE, https://perma.cc/6VPT-YCL6.

171. *TikTok*, 507 F. Supp. 3d at 107.

172. *Id*. at 102.

173. *Id*. at 107.

174. *See* MCI Telecommunications Corp. v. American Telephone & Telegraph Co., 512 U.S. 218, 228 (1994) (Scalia, J.) ("... [the time when a statute became law is] the most relevant time for determining a statutory term's meaning.") (citing *Perrin v. United States*, 444 U.S. 37, 42-45 (1979) ("A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning.")).

materials."[175] The Government instead focused on arguing that "informational materials" were not the targeted regulatory objects of the IEEPA order[176] – indeed, the policy concern behind the IEEPA order centrally involved the circulation of TikTok user data and metadata, probably more than the substance of amateur selfie videos. But the court noted that in fact, informational materials ("text, images, video, and audio") *were* expressly listed as regulatory objects in the Commerce Department Memorandum on TikTok, on which the Government had relied.[177]

The reality is that the IEEPA bar on restricting "informational materials" is extraordinarily broad – the restriction applies to "direct[] or indirect[]" prohibitions, "whether commercial or otherwise," and irrespective of "format or medium of transmission." This breadth reflects the unanimous support for the Cold War and pre-IT era policy that free information flow represents an antidote to totalitarian closed societies. Given this textual breadth, the Court's holding is understandable. However, at the same time, the obvious threats posed by foreign mass-collection of US person data makes the Court's application of the "informational materials" restriction difficult to accept. As the government remarked before the court's September 7 decision, "it is unfathomable that Congress intended through section 1702(b) to limit the President's ability to prevent a foreign government . . . from dominating the country's data services. Yet that absurd conclusion would necessarily flow from interpreting subsection (b)(3) in the way Plaintiffs suggest."[178]

Although the government conceded that TikTok videos and content constituted "informational materials," we aver that the complex nature of the TikTok *application*, and the resulting media environment, might benefit from closer analysis. While the individual videos hosted on the application might reasonably constitute "informational" materials, would the definition also encompass the software, analysis and processing, and associated metadata also include "informational materials"? As we have explained elsewhere, while individual videos on TikTok have their own intrinsic monetary value, the true revenue stream for TikTok comes not from the intrinsic value of the media it hosts, but rather from the billions of data processing transactions that occur in the background, and that presumably have little to no import to Congressional aim of keeping the free flow of information to Communist countries. Additionally, it seems apparent that the court may not have fully considered the additional contents and means of processing of data contained on the application. To extend the court's analogy—would Congress have intended for millions of ordinary Americans to jot down notes and paste photographs of other people into the margins of a news article and to send it to their pen pal in Moscow? The *TikTok* decision offers no clues,

175. *TikTok v. Trump*, 507 F. Supp. 3d at 108 ("The government does not claim that the information shared on TikTok falls outside the meaning of the phrase 'information or informational materials.'").

176. *Id.* at 109.

177. *Id.*

178. *TikTok v. Trump*, 490 F. Supp. 3d. 73, 82 (D.D.C. 2020).

and leaves one to speculate further about whether this legal framework has grappled with the true extent of TikTok's data processing activities.

* * *

In summary, the *TikTok v. Trump* decision recognized that Chinese bulk data collection represented a threat and that TikTok (and by connection ByteDance) are prolifically engaged in such collection, including contractual relationships binding them to provide such information to the Chinese Communist Party. But the court granted the injunction anyway because of the text of the IEEPA statute, illustrating that IEEPA does not represent a clear legal answer to the challenge of foreign bulk data collection.

In the aftermath of the D.C. District Court's grant of the injunction, the Trump administration continued to issue IEEPA orders to restrict Chinese companies tied to the Chinese military-industrial complex. In November 2020, the Administration issued (IEEPA) Executive Order 13959, coordinated with a 1999 National Defense Authorization Act mechanism to prohibit any U.S. investments in declared "Communist Chinese military companies" identified by the DoD. This mechanism was amended on January 13, 2020, mandating U.S. divestment from companies included on the list by November 11, 2021.[179]

PART 4: BULK DATA TRADE REGULATION—LOOKING AHEAD

With the *TikTok v. Trump* decision's interpretation of IEEPA, where might possible data trade regulation go from here? The 2020 presidential election was pivotal with respect to administrative national security regulatory mechanisms such as IEEPA and CFIUS because they are discretionary.

As the end of the Trump administration neared, former NSA General Counsel Stewart Baker interpreted the Administration's strategy toward foreign data collection as attempting to mobilize as many legal devices as possible to deny Chinese access to U.S. capital markets and data; this strategy, according to Baker, had the ostensible dual benefit of (A) withstanding independent legal challenges to the policies, some of which are at least somewhat unprecedented and (B) cementing the policies so that if then-President-elect Biden opposed the policies, he would have to expend political capital to reverse them.[180] This reflects the aforementioned reality that such policies are discretionary and may be instigated or withdrawn without legislation.

In a September 2019 appearance on the ChinaTalk podcast, Jake Sullivan—a veteran of the Obama administration and soon-to-be National Security Advisor to President-elect Joe Biden—was pressed about the purported de-prioritization of China's adversarial behavior toward the United States during

179. *Trump Bolsters Ban on U.S. Investments in China*, REUTERS (Jan. 13, 2021, 8:06 PM), https://perma.cc/7S97-2GGS.

180. Stewart Baker, *Trump's Multiple Re-Entry China Policy Vehicles*, LAWFARE (Nov. 17, 2020), https://perma.cc/4D2G-EJZY.

the Obama administration.[181] Sullivan stated that indeed, during the second Obama term, China had been less of a focus in part "because Secretary [of State] Kerry was rightly focused on the trying to close the Iran Nuclear Deal and the Paris Climate Agreement."[182]

Surprisingly, Sullivan did not discuss Chinese foreign economic collection against the United States, despite the massive annual losses to such collection during the Trump administration (which most would agree applied maximal pressure with respect to such issues).

Sullivan's lack of emphasis on foreign economic collection was not lost on former National Security Adviser Lieutenant General H.R. McMaster, who appeared on the same podcast shortly after listening to the Sullivan episode.[183] Responding to Sullivan's summary of U.S.-China policy, McMaster stated, "If you hate Donald Trump enough . . . you begin to think that [the United States] is the main determinant in the nature of this relationship. I think that's a profoundly narcissistic approach."[184] McMaster read Sullivan as implying that Trump's policies and conduct were responsible for Chinese foreign economic collection, which McMaster regarded as "self-referential."[185]

Sullivan's big-picture framing of U.S.-China tensions and the support for a tough policy toward China was particularly interesting. Sullivan suggested that with the 9/11 attacks, public sentiment had driven the policy reforms which followed, and national security and foreign policy insiders remained calm relative to popular opinion.[186] Conversely, Sullivan noted, the American public does not view Chinese activities as a major threat, while the policy community is on high alert.[187] Hence, Sullivan predicted, the U.S. stance toward China moving forward will depend partially on whether ostensible damage caused by China translates into U.S. public sentiment, driving policy makers.[188]

This final section of the article now examines, in-depth, a range of legal and policy options that the U.S. government could use to address the national security risks of cross-border data trade in personal data.

---

181. Jordan Schneider, *Incoming NSA Jake Sullivan on an Alternative Vision for US-China Relations*, CHINATALK (Sep. 2019), at 3:00-5:00 https://perma.cc/H9BW-SNTQ.

Q: (Schneider to Sullivan): "What percentage of headspace did China occupy in the Obama Administration? Do you think in retrospect it was over or under-represented?" (3:00).

Q (Schneider to Sullivan): "Over the past few years there's been a real dramatic hardening of opinion on both sides of the aisle with respect to China policy and you say that you give the [Obama] Administration 'high marks' but there's definitely a line of argument out there saying that the Obama Administration was sort of slow on the uptake, that engagement and this whole sunny lands viewpoint was actually sort of a fool's errand, and that the US should have recognized the changing nature of the Xi regime much earlier than it did. Why do you not buy into this?" (5:00).

182. *Id.* at 03:55.

183. *See* Jordan Schneider, *H.R. McMaster on China*, CHINATALK (Nov. 30, 2020, 5:01 AM), at 16:30 https://perma.cc/4F43-6MR2.

184. *Id.*

185. *Id.*

186. Schneider, *supra* note 183, at 22:00-27:00.

187. *Id.*

188. *Id.*

A. Appraising "Value" in the Current Security Environment

It is worth returning back to the D.C. District Court's *TikTok v. Trump* decision and its implicit rejection of the U.S. government's appraisal of the level of harm posed by TikTok's data collection and dissemination practices vis-à-vis China. While the court dedicated only a few paragraphs to examining whether the data exchanged comprised "things of value," it did not seem to heavily weigh the findings in the Department of Commerce Memorandum. The executive branch usually enjoys broad deference from courts on the executive's characterization of the facts regarding a national security issue.[189] But even if courts should lean against such deference, as Professor Robert Chesney outlines in his article on national security fact deference, the specific facts of the *TikTok v. Trump* decision put the judiciary in an awkward position: on what basis is the court able to put aside the executive branch's assertion that TikTok posed a foreign espionage threat?[190]

The *TikTok* court's narrow view of "value" also complicates matters further. While the legislative history of IEEPA shows a focus on monetary value, it is also worth noting that the actual IEEPA text does not reflect this. And some things are more important than money. The information passed through TikTok has great value to the Chinese security apparatus. As described in the Department of Commerce's Memorandum, TikTok is "building massive databases of Americans' personal information" to help the "Chinese government to further its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment."[191] This includes, as the Memorandum notes, the training of facial recognition and voice recognition algorithms.[192] Furthermore, TikTok utilizes data storage and processing services provided by another Chinese tech giant, Alibaba, which remains subject to Chinese laws regarding intelligence and law enforcement access despite its complicated relationship with the Chinese government.[193] Radio Free Asia reports that activists in China have grown increasingly concerned with the Chinese government's monitoring of audio content, which includes the use of audio file comparisons to ascertain speakers' identities.[194] In the words of one activist, surnamed Ding, "[The Chinese government is] tightening controls yet again … Their next step will be to go after Tencent, and then to nationalize Alibaba."[195] This prediction may have already started to come true because the Chinese government has

189. Robert M. Chesney, *National Security Fact Deference*, 95 VA. L. REV. 1361, 1362 (2013).

190. *Cf. Id.* at 1375.

191. *TikTok*, 507 F. Supp. 3d 92, 98 (D.D.C. 2020).

192. *Id.* at 99.

193. *Id. See also What's Behind China's Crackdown on its Tech Giants*, BLOOMBERG NEWS (Nov. 13, 2020, 4:40 AM), https://perma.cc/5DMB-DNJ2.

194. *See* Qiao Long, Chingman, & Gigi Lee, *China Clamps Down on Software Used to Disguise Voiceprints*, RADIO FREE ASIA (Mar. 18, 2021) (Luisetta Mudie trans.), https://perma.cc/4H5A-KJ78.

195. *Id.*

reportedly imposed additional data security requirements on Tencent's move to privatize Sogou, the third largest search engine in the Chinese market.[196]

The risk of foreign adversaries' growing interest in biometric technology and biometric data becomes especially concerning in light of the proliferation of dual-use technologies, such as DNA analysis, which happens to span law enforcement, healthcare, and even military applications—to include the potential creation of "super-soldiers" as warned by John Ratcliffe, the then-Acting Director of National Intelligence.[197]

Despite all of these dangers, the *TikTok v. Trump* court still concluded that the information passed through TikTok did not constitute a "thing of value" even though voices with interests as divergent as the U.S. Intelligence community and the ACLU have warned of the harms that may result from personal data being placed in the hands of the Chinese government or companies beholden to it.

B. Legal Aftermath of TikTok v. Trump*: Moving Toward the Export Control Reform Act ("ECRA")?*

Setting aside policy questions relating to confronting China, *TikTok v. Trump* illustrates that the pertinent legal mechanisms cannot be cleanly amplified (as they currently stand) to fight the foreign adversarial collection of U.S. person data in bulk. First, IEEPA as drafted appears to contain pivotal textual flaws rendering IEEPA's applicability (based on a plain text reading) questionable. Second, CFIUS authorities may be invoked to pre-empt data access through foreign investments in companies holding the data, but companies have the capacity to sell or circulate the data, enabling foreign collection in any case. Third, alongside CFIUS, the FTC *does* track data usage, circulation, and transactions, but the FTC cannot easily complement CFIUS's investment reviews because (1) an expanded, national-security oriented role for the FTC in policing data circulation would run afoul of the FTC's reported functions in practice; (2) related, the FTC does not recognize a "national security" role and has no reported links to CFIUS; and (3) even if the FTC reversed course and embraced a national security data trade supervisory role, it reportedly lacks the funding and logistical capacity to follow through.

The apparent reality that CFIUS and IEEPA cannot be cleanly applied to answer foreign adversarial data collection threats is highlighted by the fact that this is the case even despite *Dames & Moore*. As noted above, *Dames & Moore* holds that such mechanisms are "supported by the strongest presumption and widest latitude of judicial interpretation," where a rejection on constitutional grounds would mean that the "federal government as a whole lack[s] the power exercised by the President."[198]

---

196. *See* Pei Li & Julie Zhu, *Exclusive-China Set to Clear Tencent's $3.5 Billion Sogou Deal Subject to Sata Security Conditions - Sources*, REUTERS (Apr. 9, 2021, 1:55 PM), https://perma.cc/9XK2-6KY2.

197. *See* John Ratcliffe, Opinion, *China is National Security Threat No. 1*, WALL ST. J. (Dec. 3, 2020, 1:20 PM), https://perma.cc/HM43-8E6B.

198. Dames & Moore v. Regan, 453 U.S. 654, 674 (1981) (citing Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 636-37 (1952) (Jackson, J., concurring)).

Stewart Baker, one of the leading voices in the field, has opined that he prefers the CFIUS framework to IEEPA, which he regards as deeply flawed. But Baker also maintains that the FTC is merely "good at shooting the wounded," or in other words, lacks the capacity to hold formidable transgressors accountable.[199]

On April 15, 2021, the *Washington Post* reported that, based on concerns about data flow to adversarial countries, Senator Ron Wyden was proposing the "Protecting Americans' Data From Foreign Surveillance Act."[200] Perhaps recognizing that neither the CFIUS/(FTC) framework nor IEEPA was conditioned to be applied to regulate data for national security purposes, Senator Wyden's proposal relied instead on ECRA.

The mission statement of ECRA is found under 50 U.S.C. § 4811, which explains:

The following is the policy of the United States:

> To use export controls only after full consideration of the impact on the economy of the United States and only to the extent necessary—
>
> (A) to restrict the export of items which would make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the national security of the United States; and
>
> (B) to restrict the export of items if necessary to further significantly the foreign policy of the United States or to fulfill its declared international obligations.[201]

The term "items" would not appear to undermine Senator Wyden's proposal because the definition of "items" is "commodity, software, or technology."[202] Data would imaginably qualify as a "commodity."

The *Washington Post* coverage reported:

> The export-license requirements would apply only to countries designated as potential security threats, based on the countries' data-protection and surveillance laws; whether they had conducted "hostile foreign intelligence operations" against the United States; and the extent to which the countries' governments can "compel, coerce or pay" people within the country to hand over personal data.[203]

199. Stewart Baker, *Steptoe Cyberlaw Podcast - Interview with Dmitri Alperovitch*, STEPTOE & JOHNSON (May 17, 2016) at 18:00, https://perma.cc/87UG-8TS4.

200. Drew Harwell, *Wyden Urges Ban on Sale of Americans' Personal Sata to 'Unfriendly' Foreign Governments*, WASH. POST (Apr. 17, 2021, 7:00 AM), https://perma.cc/6KF6-ACWC.

201. 50 U.S.C. § 4811.

202. 50 U.S.C. § 4801(7).

203. Harwell, *supra* note 200.

Barring data from China as an "export" would imaginably generate significant upheaval because of the amount of trade it would constrain. First, as noted above, the new Chinese Personal Information Protection Law ("PIPL") effectively declares that any restrictions on Chinese access to data will be answered by reciprocal restrictions. Second, because ECRA (and Export Law before ECRA) regulates "reexport[ation],"[204] this would mean that the private sector would have to take measures not only to avoid circulating data to China directly but also as a secondary step: for instance, Twitter would have to prevent U.S. data sent to Korea, Japan, and Pakistan from being subsequently transmitted to China. Also, there would remain additional ethical, logistical, and constitutional questions about the consequences of walling off data from China, which could imaginably isolate Chinese and Chinese-Americans in the United States from friends and relatives in mainland China.[205]

Therefore, perhaps the overarching dynamic is the collision between administrative national security law-based regulatory mechanisms and gargantuan private sector interests. Theoretically, mechanisms such as IEEPA, CFIUS, and ECRA, as well as other statutory authorities,[206] confer almost unlimited government authority to confiscate enormous business and profit interests under the aegis of national security. The constraints on this authority (if any) are reflected in the *Dames & Moore* majority and dissenting opinions, wherein Justice Rehnquist, writing for the majority, held that "such orders permit the President to maintain the foreign assets at his disposal for use in negotiating the resolution of a declared national emergency. The frozen assets serve as a 'bargaining chip' to be used by the President when dealing with a hostile country."[207] Justice Powell, dissenting, expressed concern about foreign assets as "bargaining chips," which he felt ought to bind the government to pay just compensation to foreign adversarial parties holding such assets.[208]

---

204. *See* 50 U.S.C. § 4811(2).

205. *See* U.S. WeChat Users All. V. Trump, 488 F. Supp. 3d 912, 927 (N.D. Cal. 2020) ("[P]laintiffs establish through declarations that there are no viable substitute platforms or apps for the Chinese-speaking and Chinese-American community. The government counters that shutting down WeChat does not foreclose communications for the plaintiffs, pointing to several declarations showing the plaintiffs' efforts to switch to new platforms or apps. But the plaintiffs' evidence reflects that WeChat is effectively the only means of communication for many in the community, not only because China bans other apps, but also because Chinese speakers with limited English proficiency have no options other than WeChat.").

206. *See, e.g.*, the NIST Act, 15 U.S.C. § 271. The stated "purpose" of the NIST Act is safeguarding and supporting commercial activity in the United States, including "public safety." 15 U.S.C. § 271(b)(1). Therefore, the Act authorizes the Secretary of Commerce to "take all actions necessary and appropriate to accomplish the purposes of this Act," which includes formulating standards and "implementation activities." 15 U.S.C. § 272. With respect to "computer standards" particularly, the NIST Act stipulates that "In general . . . the institute shall have the mission of developing standards, guidelines, and associated methods and techniques for information systems." 15 U.S.C. § 278g-3(a)(1). "Information systems" is a widely used legal drafting term encompassing computers and computer technology. 15 U.S.C. § 278g-3(f)(3) (citing 44 U.S.C. § 3502(8)).

207. Dames & Moore v. Regan, 453 U.S. 654, 673 (1981).

208. *Id.* at 690-91 (Powell, J., dissenting).

Iran's contractual obligation to Dames & Moore for the firm's work in Iran was $3 million (almost $10 million adjusted for inflation in 2022). But TikTok is a $400 billion company and is by no means the only Chinese tech conglomerate tied to the CCP and operating within the United States. Even if acting in reliance on properly delegated congressional authority, a presidential order confiscating or banning such entities runs not merely into legal questions about applying *Dames & Moore*, but further may collide with the democratic process itself. Indeed, this may explain why Senator Wyden proposed legislation to construe U. S. person data as an "export" under ECRA, even though ECRA may provide such authority as it currently stands. In short, the stakes of such maneuvers are so high for both the private sector and consumers that even though administrative national security law confers authority to partially or fully divest a company controlled by an adversarial foreign country, such authority cannot be exercised without full U.S. democratic and legislative proceedings.

C. Potential Alternatives to IEEPA: EAR and Data Controls

Another potential future regulatory battleground for restricting foreign adversarial access to data is the Export Administration Regulations ("EAR").

Currently, the export controls regime overseen by the Department of Commerce regulates the foreign transfer of some biometric technology.[209] This regime, however, does not address underlying data—in fact, it likely excludes such data from its scope because the purposes of the EAR appear to focus primarily on physical items, particularly armaments and munitions.[210] If amended, the U.S. export controls regime could provide a helpful way to balance competing economic and security interests, given that its licensing practice already permits some exports for research and other purposes.[211] But if existing authorities such as IEEPA or CFIUS do not reach the exchange of personal data, then using the EAR does not seem viable.[212]

Furthermore, data may actually fall outside the scope of the EAR, which covers the export and use of "items," which in turn means "commodities, software,

209. The Export Administration Regulations (EAR) include fingerprint, voice, and DNA technologies, but do not include other biometric modalities like facial recognition or iris recognition. *See* U.S. DEP'T OF COM., COM. CONTROL LIST, Entry 4A980 (2009).

210. 15 C.F.R. § 730.6 ("Some controls are designed to restrict access to items subject to the EAR by countries or persons that might apply such items to uses inimical to U.S. interests. These include controls designed to stem the proliferation of weapons of mass destruction and controls designed to limit the military and terrorism support capability of certain countries.").

211. *Cf.* Ari Schwartz, *Standards Bodies Are Under Friendly Fire in the War on Huawei*, LAWFARE (May 5, 2020, 8:00 AM) https://perma.cc/Z3UD-AXXN ("The United States can pursue its national security concerns with companies like Huawei via the Entity List without the need to silence American voices in vital standards development efforts. The Bureau of Industry and Security can easily provide guidance that leaves Huawei on the Entity List while it allows U.S. companies to engage in SDOs where Huawei is trying to gain a foothold.").

212. *See* 15 C.F.R. § 730.2 (discussing use of Export Administration Act and IEEPA as statutory authority for the EAR).

or technology."[213] Clearly, data itself could not constitute "software," which means a program or microprogram.[214] "Technology" is more plausible. The EAR defines technology as "[i]nformation necessary for the 'development,' 'production,' 'use,' operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control 'technology') of an item."[215] The EAR goes on to explain that "technology" can take any tangible or intangible form, which, critically for biometric information such as facial recognition, explicitly includes photographs.[216] This definition, while helpful for demonstrating coverage under the EAR for ordinary personal data that social media apps can collect, is hopelessly circular. Characterizing data as a "commodity" might have better luck, as the EAR defines the term as "any article, material, or supply" that would not fall into technology or software.[217] While the EAR does not supply a definition of "article" or "supply," the term "material" means "any list-specified crude or processed matter that is not clearly identifiable as any of the types of items defined in § 772.1 under the defined terms, 'end item,' 'component,' 'accessories,' 'attachments,' 'part,' 'software,' 'system,' 'equipment,' or 'facilities.'"[218] Raw data, including photographic images, does not appear on the Commerce Control List. Nor would data, in an electronic format, constitute "matter"—the EAR appears to focus its "materials" on tangible things.

But the *TikTok* decision also mounts a major obstacle to the use of the EAR to stop foreign adversarial data transfers: the EAR makes clear that while the Export Administration Act of 1979 ("EAA") provides the primary source of authority for the EAR, should the EAA lapse, the President can continue to operate the export controls regime using IEEPA.[219] An unofficial compilation of authorities from the lawyers at Commerce's Bureau of Industry and Security explains why the *TikTok* decision would impede the application of the EAR:

> "the authority under this Part may not be used to regulate or prohibit under this part the export . . . of any item that may not be regulated or prohibited under [50 U.S.C. § 1702(b)]."[220]

Thus, the TikTok decision (A) deprives the U.S. government of another tool in the national security toolbox to stop harmful data transfers, but also (B) deprives industry of a potential off-ramp whereby the government could use a robust and more consultative licensing regime to approve certain transfers, setting the course for a serious collision between security and commercial interests.

213. 15 C.F.R. § 772.1 (providing definitions used in the EAR).
214. *Id.*
215. *Id.*
216. *Id.*
217. *Id.*
218. 15 C.F.R. § 772.1 [emphasis added].
219. 15 C.F.R. § 730.2.
220. OFF. OF THE CHIEF COUNS., BUREAU OF INDUS. AND SEC., LEGAL AUTHORITY (2020).

PART 5: CASE IN POINT—STAKES OF DATA TRANSACTABILITY FOR THE MUSIC BUSINESS

In Part 5, we examine the other side of foreign cross-border transfers of personal data, including sensitive data, namely from the perspective of industry. As suggested above, not only does the *TikTok* decision constrain government action in the interest of national security, but it may also lead to uncertainty in the private sector and negative consequences for corporate revenue. In this penultimate section, we examine the stakes for industry by looking at data transfer practices in the music business.

The exponential rise in the value of data is an established fact. The private sector practice of transacting with a consumer by acquiring their data rather than requesting payment via currency is today widespread.[221] Furthermore, as noted above, the data brokerage industry is booming—in 2020, data broker lobbying expenditures resembled that of big tech companies such as Google and Meta.[222] Indeed, many industries now financially depend on data trade and fungibility. Perhaps one of the most dramatic illustrations of this phenomenon is the trajectory of the recording industry.

Revenue from recorded music reached a peak of $22.4 billion in 1999.[223] However, the rise of piracy and file sharing hurt the recording industry—consumers had little reason to pay for music when they could download tracks for free. Those who did purchase CDs had few qualms about inserting them into a computer disc drive and circulating the files to friends. Beginning in the early 2000s, recording industry growth slowed, then dropped to negative seven to eight percent all the way through 2009 and did not move above zero until 2012.[224] By 2015, growth had finally increased to three percent, but total revenue had fallen to only $6.9 billion—one-third of revenue in the late '90s.[225] These numbers appear readily traceable to piracy and file sharing because, for instance, the percentage of household entertainment expenditures on music dropped from seven and a half percent in 1998 to under four percent from 2008-2014, before beginning to increase again.[226] Finally, as of 2019, recording industry revenue has climbed back to $11.1 billion.[227]

These statistics raise questions about what, specifically, enabled the recovery of the music business in the mid-2010s. Streaming revenues imaginably increased

221. *See, e.g.*, Thierry Rayna, John Darlington & Ludmila Striukova, *Pricing Music Using Personal Data: Mutually Advantageous First-Degree Price Discrimination*, 25 ELEC. MKTS. 139, 144 fig.2 (2015), https://perma.cc/D935-ACCX.

222. Ng & Varner, *supra* note 11.

223. Dylan Smith, *Despite Streaming, US Recorded Music Revenues Still Down 50% from 1999 Peaks*, DIGIT. MUSIC NEWS (Aug. 27, 2020), https://perma.cc/7U6F-UX82.

224. Lisa Yang, Heath Terry, Masaru Sugiyama, Simona Jankowski & Heather Bellini, *Music in the Air: Stairway to Heaven*, GOLDMAN SACHS 1, 13 (Oct. 4, 2016), https://perma.cc/U66L-XRYE.

225. Nick Routley, *Visualizing 40 Years of Music Industry Sales*, VISUAL CAPITALIST (Oct. 6, 2018), https://perma.cc/5GDA-EUYY.

226. Yang et al., *supra* note 224, at 11.

227. Smith, *supra* note 223.

over time because streaming (and music consumption generally) has been channeled into platforms such as Spotify and YouTube, which formally license music from record labels. The drastic decline in physical sales and pivot to streaming have also reduced the proportion of music consumers hold independently on their computers and can freely circulate. However, the rise of the major streaming platforms cannot fully account for revenue recovery—streaming royalties themselves pale in comparison to the profits of selling each individual consumer LPs and CDs, adjusted for inflation.[228] For this reason and others, it seems a fair inference that the economic recovery of the music industry hinges significantly on data innovation.

While it would seem difficult to trace precisely how and when the music industry began incorporating bulk data collection and exploitation into its practices, there are sources that can trace these progressions as arising essentially in the past decade. For example, a 2011 "Digital Distribution Agreement" between Sony and Spotify—made available in the public domain—included a full subsection addressing data rights. The agreement bound Spotify to provide user streaming data to Sony both in real-time and in reports.[229]

Thus, generally, big data technology seems to have invigorated the music business on both novel and traditional fronts. In some cases, data innovation enables new music business mechanisms which would not have been possible years ago. At the same time, data technology seemingly amplifies and supports existing music business tools. An example of the former would be social media marketing campaigns loosely based on the traditional phenomenon called "Payola," but bolstered by data innovation.[230] Examples of the latter might include the data collection and rights now arranged as part of licensing agreements and the capacity to use data technology to expeditiously identify intellectual property and ensure royalty payments.

In 2021, Ethan Baer, Co-Founder of Rebel Creator Services ("Rebel"), a music and marketing firm that runs data-driven marketing campaigns for some of the biggest recording artists and record labels in the world, successfully developed a Payola-inspired campaign to promote the artist Saweetie, and her new song, "Best Friend."[231] Baer's strategy had two prongs: he paid YouTube to have "Best

228. *See, e.g.*, *Music Streaming Overtakes Physical Sales for the First Time – Industry Body*, REUTERS (Apr. 24, 2018), https://perma.cc/7ZEN-EKHD.

229. Sony and Spotify, Digital Distribution Agreement 39-40 (2011).

230. "Payola" is the name for the old, illegal practice of paying a radio station to play songs without the station disclosing that the song was being broadcast in exchange for financial compensation. The applicable statute, stemming from the Communications Act of 1934, requires disclosure (announcement) of payments made to "radio stations." 47 U.S.C. § 508. "Radio station" is a term defined under the Act as "a station equipped to engage in radio communication or radio transmission of energy." 47 U.S.C. § 153. Despite this seemingly narrow drafting language, Spotify and YouTube both apparently construe the statute as applicable to streaming and therefore label "Sponsored Content." Dani Deahl, *Spotify is Testing 'Sponsored Songs' in Playlists*, THE VERGE (June 19, 2017), https://perma.cc/AX2F-TZUD.

231. Saweetie, *Saweetie - Best Friend (feat. Doja Cat) [Official Music Video]*, YOUTUBE (Jan. 7, 2021), https://perma.cc/HY4F-KRC9.

Friend" play as an ad displaying to pre-qualified YouTube subscribers – identified through data analytics as likely to engage with and be interested in the song.[232] Then, separately, Baer arranged for a contemporaneous marketing campaign designed around generating direct, organic viewership to complement the paid media strategy: Baer and his team secured a partnership with Tesla, whereby they donated two new cars to be offered as part of a giveaway—eligibility to win a free Tesla required users to submit an email address, subscribe to Saweetie on YouTube, and leave a comment on her video for "Best Friend."[233] The campaign successfully engaged over eleven million registrants who completed the required actions so that "Best Friend" quickly accrued over 100 million views, now at 238 million as of this writing.[234] Beyond this dramatic spike in YouTube streams, the giveaway generated yet further value through registrations because the giveaway module was designed so that registrants—the apparent "audience pool" for Saweetie and similar music—could be subsequently tracked and targeted with advertising as they browsed the internet.[235]

According to Baer, these data-driven promotional music initiatives are valued based on the mathematically-calculated gross aggregate value of anticipated saturation of the promoted song and artist across all digital music platforms, plus the value of the data itself.[236] Because digital music companies today can anticipatorily value data, the investment was a relatively low-risk decision; accordingly, Baer calculated that the data developed from and by the eleven million registrants would eclipse the value of the advertising spend and that of the two Tesla cars.[237] Transposed to a traditional music business atmosphere (during the twentieth century, for example), there were no "user comments" and "subscriptions," which could be rapidly solicited to almost immediately reimburse and exceed the cost of giving away luxury cars (without risk).

Separately from innovations such as the Saweetie promotional campaign, one can also imagine that given the capacity of music companies to calculate and anticipate data collection and value, licensing agreements between sophisticated parties (such as the aforementioned Sony-Spotify agreement) would account for the value of whatever data might be generated from streaming the licensed content. While this might mean greater profits for both sides, it could also mean generally that companies would be more willing to negotiate such agreements, and pay advances for licenses, because of lower financial risks based on predictable expectation of value derived from data accrual, additional to streaming royalty revenue.

---

232. Zoom interview with Ethan Baer, Co-Founder of Rebel Music Services (May 16, 2021).

233. *See, e.g.*, Saweetie, *supra* note 231.

234. *Id.*

235. Baer further notes a music-specific offshoot of data brokerage: Digital music companies working with musicians employ data technology to develop specific "audience pools" (tailored to the artist), and then exploit these pools over time, cumulatively generating streaming activity and collateral revenue streams such as merchandise sales.

236. Baer interview, *supra* note 232.

237. *Id.*

Another example of how data technology seemingly amplifies and supports existing music business tools is the success of digital music companies such as Rebel. Rebel became a player in the digital music market not through music marketing and promotions; rather, they recognized that User-Generated Content ("UGC") platforms such as YouTube and TikTok collected royalty revenue for all videos but did not pay out the royalties if the UGC platform's in-house rights-matching system could not confirm the rightsholder with a ninety percent or higher match. In other words, any rightsholder whose intellectual property rights were confirmed by a probability of between one and eighty-nine percent could not collect that revenue from a major UGC platform—the revenue collected by the platform from these assets remained undistributed. Rebel uses data technology to solve the royalty matching and distribution problem on behalf of rightsholders (across all the major UGC streaming platforms such as YouTube, TikTok, and SoundCloud) and was hired as the "Claiming Partner" for dozens of major independent artists and record labels.[238]

A critical point underlying these different music business initiatives enabled or materially amplified by data innovation is that the economic viability of such initiatives is directly tied to the ease with which data may be permissibly circulated. In many cases, major consumer brands will even subsidize the cost of these marketing efforts in return for access to the user data harvested during the promotional activity. If the internet were "Balkanized"[239] and data circulation and trade constrained, this change would presumably reduce estimated data-related profits and increase investment risks, harming the digital music media market. In fact, one could move even a step further and suggest that the general recovery of the music industry in the past few years is probably tied to lenient restrictions on data transactions and usage. Therefore, the stakes for the music business and the transactability and circulation of data would seem to be extraordinarily high.

And, of course, the question of data circulation also particularly implicates questions about *international* music streaming and data flow. A 2017 Goldman Sachs report tracing the gradual recovery of the recording industry after the dark period from the early 2000s pointedly advised:

> China offers a useful case-study of a large, under-monetised music market, where streaming is opening up sizeable new monetisation avenues at a time when the value of IP is being increasingly recognised. In 2016, the Chinese music market was the 12th largest in the world (up from #14 in 2015), exceeding Sweden for the first time and recording 20% growth yoy to c.$200 mn, driven by 31% growth in streaming. Of note, streaming accounted for 84% of total recorded music revenue in 2016. According to iResearch, there were nearly 530 mn monthly active users of online music in 2016 or c.72% of the total mobile/internet population, while data from Analysis points to 720 mn

238. *Id.*

239. *See* A. Michael Spence & Fred Hu, *Preventing the Balkanization of the Internet*, COUNCIL ON FOREIGN RELS. (Mar. 28, 2018), https://perma.cc/ZF7M-LHWK.

> monthly active mobile user accounts currently (which includes users with more than one account).
>
> While the number of Chinese streaming users is already significant, the industry operates largely on a freemium model supported by advertising revenue, with optional premium subscriptions starting at RMB8, or $1.2 a month. We estimate that c.3% of monthly active mobile accounts currently pay for a music subscription. We therefore expect future revenue growth to be mainly driven by the increased conversion of users from free to pay.
>
> We believe the three major labels UMG, Sony Music and Warner Music are currently under-represented in China given the prevalence of local content and the high degree of fragmentation in the label industry. We estimate Western artists make up on average less than 10% of all music streamed across Chinese streaming platforms. That said, the majors have stated their intentions to invest and grow their market shares in China, and all three of them already have licensing deals in place with Tencent, the largest music streaming operator in China through QQ Music, Kugou and Kuwo (over 70% market share, according to IFPI). In May 2017, UMG granted the exclusive distribution of its content in China to Tencent, for which Tencent is reported to have paid an upfront fee according to Caixin (August 11, 2017).[240]

What seems surprising is that this Goldman Sachs recommendation postdates the election of Donald Trump, who assumed office in January 2017, emphatically criticizing China's foreign economic collection against the United States and asymmetrical trade policies. Also, as noted above, Tencent is one of the Chinese technology companies known – above almost all others – for Chinese nationalism and ties to the Communist Party.[241]

Amidst the uncertainty of the U.S.-China relationship during the Trump Presidency, Chinese tech companies began investing in Western music companies. In December 2017, Tencent purchased an 8.91% stake in Spotify under a "Subscription" equity agreement—an ostensibly passive investment—which subsequently reached the public domain.[242] Even though the investment was passive, Tencent represented that they would take care to avoid running afoul of U.S. Treasury Department sanctions enforcement.[243]

The degree of Chinese ownership and current legal access to U.S. data and intellectual property points toward potential conflict for the security reasons described in Part 4 above. Major tech companies such as Meta are aligned to oppose restrictions on data trade, with Mark Zuckerberg publicly suggesting that

240. Lisa Yang, Masaru Sugiyama, Heath P. Terry & Piyush Mubayi, *GS Music in the Air Series: And the Beat Goes On. . .*, GOLDMAN SACHS 1, 12-13 (Aug. 28, 2017).

241. *See, e.g.*, Keoni Everington, *Caught Red-Handed: Tencent's Ties to the CCP Revealed*, TAIWAN NEWS (Aug. 14, 2020), https://perma.cc/2AJB-C3RU.

242. Tencent Music Entertainment Group, 2017 Tencent-Spotify Subscription Agreement (2018).

243. *Id.*

privacy itself is no longer a social norm.[244] Cutting in the other direction, the influence of the EU's GDPR has spurred U.S. states gradually to adopt GDPR-inspired restrictions on data trade, with California being the most prominent example.

CONCLUSION

Reporting in June 2021 confirmed that TikTok continued to funnel US person data to China *en masse* – former TikTok employees stated that the boundaries between TikTok and Bytedance were "so blurry as to be almost non-existent."[245] This was further corroborated by leaked audio from internal TikTok meetings in which, for example, a member of TikTok's Trust and Safety department stated that "everything is seen in China."[246] In June 2022, TikTok announced an agreement to route its American users' data to US-based servers owned by Oracle.[247] However, as of November 2022 it appears that broad Chinese access to US person TikTok data continues.[248]

The national security challenges posed by foreign adversarial bulk data collection of U.S. person data, such as those examined in the FaceApp use case, are relatively new and have emerged as a function of the continuing progress of data processing technology. These challenges implicate national security regulatory frameworks – IEEPA and CFIUS – which are theoretically applicable but also not cleanly aligned. IEEPA was passed before the digital era, and with *TikTok v. Trump*, its applicability to address the issues discussed in this article seems uncertain. CFIUS has been updated in part to address foreign bulk data collection, but parties seeking U.S. person data do not need to invest in U.S. companies to access such data—they can buy it from data brokers. In theory, approaching foreign bulk data collection challenges through CFIUS might be regarded as workable in tandem with the FTC's data trade-in-practice oversight; however, the FTC disclaims a national security role.

The appearance that IEEPA and CFIUS do not foster a clear legal and regulatory response to foreign bulk data collection was corroborated by *TikTok v. Trump* and is yet further evident given (A) the degree of deference afforded these mechanisms by *Dames & Moore v. Regan* and (B) the fact that Congress is

244. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010), https://perma.cc/ZY8Q-JDQ2.

245. Salvador Rodriguez, *TikTok Insiders Say Social Media Company is Tightly Controlled by Chinese Parent Company Bytedance*, CNBC (June 25, 2021), https://perma.cc/M2CT-KAAY.

246. Elizabeth Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, BUZZFEED NEWS (June 17, 2022, 12:31 PM), https://perma.cc/K9Y2-CMYE.

247. Manish Singh, *TikTok Moves All US Traffic to Oracle Servers, Amid New Claims User Data was Accessed from China*, TECHCRUNCH (June 17, 2022, 2:33 PM), https://perma.cc/E4F7-DRDS;

Emma Roth, *TikTok and Oracle Teamed up After All, But Concerns About Data Privacy Remain*, VERGE (June 19, 2022), https://perma.cc/M2WW-6V6U.

248. Christianna Silva & Elizabeth de Luna, *It Looks Like China Does Have Access to U.S. TikTok User Data*, MASHABLE (Nov. 3, 2022), https://perma.cc/HBA9-S7KV.

contemplating alternative legislation outside of IEEPA and CFIUS, such as under ECRA.

Finally, even if these review and regulatory mechanisms were more definitively tailored to addressing foreign bulk data collection, there remains the complication of overwhelming private sector interests in unrestricted data trade. TikTok is worth $400 billion, and individual videos and NFTs can yield hundreds of thousands of dollars. There are entire industries whose profitability now depends on data trade and fungibility. Any major response to the threats posed by foreign bulk collection of U.S. data—either through existing frameworks or through new legislation—is yet more challenging because it must account for these overwhelming private sector financial interests.

Especially given the calls for ECRA regulation through legislation and the scope of the industry stakes, Jake Sullivan may be correct that the disputes over cross-border data trade and U.S. data privacy will be decided in the court of public opinion. While the U.S. government has expressed grave concerns about the export of personal data to countries like China, it is not clear what the American public believes or desires. Moreover, unfortunately, the public debate over data use and governance has devolved into a quagmire of shifting and inconsistent positions that change depending on what kind of data is being made available and who seeks it. The problem of the sharing, sale, and transfer of data across borders and between companies is so monumental that it is difficult to overstate. The *TikTok* decision makes solving these problems even harder.

***