ARTICLE

THE PRESIDENT'S AUTHORITY OVER CROSS-BORDER DATA FLOWS

ANUPAM CHANDER† & PAUL SCHWARTZ††

This Article reveals a surprising expansion of presidential authority to control goods and services available in the United States because of the information flows that they entail. Such authority is grounded in laws focused on protecting national security, here with respect to foreign surveillance and propaganda. But broad executive powers over our information infrastructure raises significant concerns with respect to core American values of free expression and due process. Worries about unfettered foreign access to data should be coupled with worries about unfettered executive control over our information services and technologies.

INTRODUCTION 1990
I. ASSERTING PRESIDENTIAL AUTHORITY OVER CROSS-BORDER DATA FLOWS 1994
A. *The TikTok Challenge: High Noon on Capitol Hill* 1995
B. *IEEPA and Personal Data* 1999
1. The Road to the "Informational Materials" Exclusion 2000
2 Ensuring Free Trade in Ideas: The Berman Amendment and Free Trade in Ideas Act.....2001

† Scott K. Ginsburg Professor of Law and Technology, Georgetown Law Center; Visiting Scholar, Institute for Rebooting Social Media, Harvard University. For their comments and suggestions, the authors would like to thank Elena Chachko, Erwin Chemerinsky, Danielle Citron, Kristen Eichensehr, and Katrina Linos. The authors also thank our helpful student editors at the University of Pennsylvania Law Review: Ecclesiaste Desir, Elizabeth Dowdle, Bryce Klehm, Danielle Moore, and Jonathan Wiersema. We are grateful as well for the assistance of Professor Schwartz's research assistants, aka "Team Privacy": Ryan Campbell, Saabhir Gill, Kiana Harkema, and Emma Neukrug, as well as Professor Chander's research assistants, Donara Aghajani and Caroline Manning .

†† Jefferson E. Peyser Professor of Law, Berkeley Law School.

C. *CFIUS and Personal Data* 2004
D. *The TikTok Law and Personal Data* 2006
E. *Executive Orders and Regulations* 2010
II. CONSTRAINING PRESIDENTIAL AUTHORITY OVER CROSS-BORDER DATA FLOWS 2017
A. *IEEPA, CFIUS, the TikTok Law, and the Rise of Group Privacy* 2018
1. Open Questions Under IEEPA, Ample Power Under CFIUS and the TikTok Law 2018
2. Defining Personal Data: A Confused Mixture 2021
3. The National Securitization of Personal Data 2024
B. *Statutory and Constitutional Constraints* 2031
1. Statutory Constraints 2031
2. First Amendment Constraints and the Executive's Power over Foreign Affairs 2035
3. Due Process Constraints 2040
C. *Responding to the National Securitization of Personal Data* 2042
1. The National Security Constitution for Personal Data 2042
2. Initial Responses and Future Research 2045
CONCLUSION 2049
APPENDICES 2050
A. *Executive Orders and Regulations on Cross-border Data Flows* 2050
B. *OIS Definition of Sensitive Personal Data* 2051

INTRODUCTION

Are there limits to the President's power, statutory or constitutional, to control the flow of information across borders to protect the personal data of Americans? If so, what are these limits, and are these restrictions appropriate and adequate? These issues are front and center as the U.S. government responds to the possible national security risks of TikTok, the wildly popular short-video app that is owned by a company headquartered in Beijing.

When President Donald Trump attempted to ban TikTok in 2020, his ban floundered when lower federal courts deemed it ultra vires.[1] To President Trump's chagrin, decades earlier, Congress had explicitly excluded the authority to control the transfer across borders of "informational materials" from the President's power to respond to international peacetime

1 *See* TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 115 (D.D.C. 2020) ("Here, . . . the government likely exceeded IEEPA's express limitations . . . ."); Marland v. Trump, 498 F. Supp. 3d 624, 641 (E.D. Pa. 2020) ("Plaintiffs . . . are likely to succeed in their argument that the Commerce Identification is *ultra vires* under IEEPA's informational materials exception.").

emergencies.[2] Thus, two federal courts wasted no time in finding that President Trump's executive order, which relied on the International Emergency Economic Powers Act (IEEPA), exceeded his statutory authority.[3]

Courts have not evaluated, however, an alternative source of Presidential authority vis-a-vis TikTok, one that Congress has explicitly provided. This source of power is the Executive Branch's long-standing authority through the Committee on Foreign Investment in the United States (CFIUS) to mitigate risks from foreign investments.[4] In 2018, Congress expanded this authority to include, for the first time, investments in firms with access to Americans' personal data.[5]

Moreover, in April 2024, Congress enacted and President Joseph Biden signed the Protecting Americans from Foreign Adversary Controlled Applications Act ("the TikTok Law"). This statute goes even further in many respects than IEEPA in terms of expanding the President's power of personal data flows to certain foreign nations.[6] The TikTok Law permits the President to designate any company in which a person from China, Iran, North Korea, or Russia has at least a 20 percent stake, and which permits information sharing by at least one million users, presumably ones located in the United States, as a "foreign adversary controlled application."[7] Upon such a designation, the company would have to effect a divestment sufficient to persuade the President that it was no longer subject to control by a foreign adversary, or else face a ban in the United States.[8] This law automatically designates TikTok as such a company requiring either divestiture or banning.[9]

Another bill before Congress, the RESTRICT Act, would extend the Executive Branch's national security review powers beyond inbound investments to offerings of goods or services by companies based in foreign

---

2 *See infra* Section I.B (discussing the evolution of the President's emergency powers).

3 *See* cases cited *supra* note 1.

4 *See The Committee on Foreign Investment in the United States (CFIUS)*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius [https://perma.cc/KDZ5-Y43J] (last visited Apr. 4, 2024) ("CFIUS is an interagency committee authorized to review certain transactions involving foreign investment in the United States . . . in order to determine the effect of such transactions on the national security of the United States.").

5 *See* Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1702(c)(5), 132 Stat. 2174, 2177 (2018) (allowing CFIUS to consider "the extent to which a covered transaction is likely to expose . . . personally identifiable information, genetic information, or other sensitive data of United States citizens to access by a foreign government or foreign person . . . .").

6 *See generally* 21st Century Peace Through Strength Act, H.R. 8038, 118th Cong. div. D (2024).

7 *Id.* § 2(g).

8 *See id.* § 2(a)(1)(B) (prohibiting foreign adversary controlled applications from "[p]roviding internet hosting services to enable the distribution, maintenance, or updating of such foreign adversary controlled application for users within the land . . . of the United States.").

9 *Id.* § 2(g)(3)(A)(ii).

countries that are deemed adversaries to the United States.[10] The RESTRICT Act also calls for the Commerce Department to prioritize national security evaluations of any services that collect the sensitive personal data of more than a million Americans through "mobile applications."[11] These measures give the President of the United States the power to shutter apps on Americans' smartphones. Similar broad powers to review digital services—and the apps Americans use—are already included within executive orders and regulations issued by the Biden administration.[12] The most recent of these executive orders will bar data brokers from selling the sensitive data of U.S. persons to organizations located in "countries of concern."[13]

This growing executive branch power over personal data reflects a major shift in national security law: congressional delegations to the Executive have transformed individual choices about personal privacy into national security issues. There has been a "national securitization" of information privacy law. Just as there is a collective interest in national security, the law now recognizes a group interest in privacy.

The resulting presidential power to control cross-border flows of personal data falls seemingly at the apex of the President's constitutional authority, as famously categorized by Justice Robert Jackson in *Youngstown Sheet & Tube Co. v. Sawyer*.[14] After all, two branches of government, Congress and the executive, have endorsed this power over personal data. Yet, even such combined exercise of power might prove unconstitutional. In his *Youngstown* concurrence, Justice Jackson observed that if the President's "act is held unconstitutional under these circumstances, it usually means that the Federal Government as an undivided whole lacks power."[15] In this case, constitutional limits on the President's powers over cross-border data flows will likely rest on the First Amendment and the Due Process Clause of the Fifth Amendment.

In examining the Trump administration's attempted bans on TikTok and WeChat, another Chinese-owned app, federal courts have already identified

10 Restricting the Emergence of Security Threats that Risk Information and Communications Technology Act, S. 686, 118th Cong. (2023) (authorizing "the Secretary of Commerce to review and prohibit certain transactions between persons in the United States and foreign adversaries").

11 *Id.* § (5)(a)(6)(B).

12 *See infra* Section I.D.

13 Exec. Order No. 14,117, 89 Fed. Reg. 15421 (Mar. 1, 2024).

14 *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring) ("When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate.").

15 *Id.* at 636-37.

constitutional restraints on executive power over cross-border data flows.[16] These cases take on new importance considering the possibility of divestiture or banning under the TikTok Law.[17] Here, we have an explicit statutory approval by Congress of the executive's power over a foreign digital company's access to the personal data of Americans.[18]

Ultimately, an overarching question in resolving the TikTok challenge is whether foreign relations exceptionalism in U.S. law should extend to personal data in cyberspace—and, if so, to what extent.[19] Existing statutes are now invoked on a bipartisan basis to support extraordinary claims of executive power over our private digital infrastructure, including the software and services that we use on a daily basis. Through the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), the statutory framework for CFIUS now gives the executive branch authority to regulate international transactions involving "personally identifiable information, genetic information, or other sensitive data of United States citizens."[20] Indeed, the history of executive branch oversight of foreign investment in the United States is one of Congress steadily increasing its grant of authority to the executive branch. The enactment of the TikTok Law in April 2024 is only the most recent example of this trend.

This Article explores the sources and limits of the executive branch's authority over foreign affairs in the information age with a focus on issues pertaining to personal data. The Article proceeds as follows. Part I chronicles

---

16 *See* Marland v. Trump, 498 F. Supp. 3d 624, 634 (E.D. Pa. 2020) (identifying the First and Fifth Amendments as possible constitutional restraints, but declining to reach these arguments because the case could be decided on ultra vires grounds); TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 112 n.6 (D.D.C. 2020) (same); WeChat Users All. v. Trump, 488 F. Supp. 3d 912, 917 (N.D. Cal. 2020) (granting a preliminary injunction on the ground that plaintiffs "have shown serious questions going to the merits of the First Amendment claim"). A federal court reached a similar conclusion with respect to a statewide Montana TikTok ban enacted in 2023. *See* Alario v. Knudsen, No. CV 23-56-M-DWM, 2023 WL 8270811, at *5 (D. Mont. Nov. 30, 2023) ("[B]ecause Plaintiffs have shown that [the Montana TikTok ban] is unlikely to pass even intermediate scrutiny, it likely violates the First Amendment.").

17 *See generally* 21st Century Peace Through Strength Act, H.R. 8038, 118th Cong. div. D (2024).

18 *See id.*

19 *See* Curtis A. Bradley, *Foreign Relations Law and the Purported Shift Away From "Exceptionalism"*, 128 HARV. L. REV. F. 294, 294 (2015) (responding to a "claim that there has been a shift away from treating foreign relations law issues as 'exceptional' toward treating them as 'normal'").

20 *See* Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1702(c)(5), 132 Stat. 2174, 2177 (2018); *see also* PRAC. L. CORP. & SEC., FIRRMA SIGNED INTO LAW, EXPANDING SCOPE OF CFIUS REVIEW (2018), Westlaw W-016-2587, https://next.westlaw.com/Document/Ifea2837ca06e11e8a5b3e3d9e23d7429/View/FullText.html?transitionType=Default&contextData=(sc.Default) [https://perma.cc/G9XA-VQ2G] (describing CFIUS's authority "over non-control investments in businesses engaged in critical technologies, critical infrastructure, or sensitive personal data").

the emergence of a complex and surprisingly broad set of statutory authorities over data, beginning with IEEPA and CFIUS and extending to executive orders and regulations issued in the last five years. Part II then analyzes the most important normative issues raised by these broad executive powers.

This Article reveals a vast expansion of presidential authority to control goods and services available in the United States because of the information flows that they entail. This vast expansion can be justified by the fact that a foreign nation's unfettered access to American personal data poses national security concerns. However, it is important to remain cautious because presidential authority in the name of national security can become a means to undermine the core American values of free expression and due process. Worries about unfettered foreign access to data should be coupled with worries about unfettered executive control over our information services and technologies.

This Article maps the still evolving landscape of this policy area. It analyzes leading statutes and the most important executive orders as well as critical normative questions about this national securitization of personal information flows. This Article explores possible statutory and constitutional constraints on the President's power over international data flows. It concludes by sketching the elements of a National Security Constitution for Personal Data: first, a requirement for specific evidence of risks before the banning or restricting of an information app on national security grounds, and second, a judicial process to test the government's claims of a foreign threat due to cross-border flows. Finally, new means are necessary to provide lawyers for regulated entities with adequate information to defend the interests of their clients.

I. ASSERTING PRESIDENTIAL AUTHORITY OVER CROSS-BORDER DATA FLOWS

What is the source of executive power over cross-border flows of personal data? This Part begins with a visit by the CEO of TikTok to a high-stakes congressional hearing on March 23, 2023 and an exploration of the policy issues aired that day on Capitol Hill.[21] The House hearing considered TikTok's impact on data privacy. Members of Congress shared bipartisan concern about the ability of this Chinese-owned company to collect and exploit the personal information of Americans and to disseminate propaganda through the app.

---

21 *See generally TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms: Hearing Before the H. Comm. on Energy & Com.*, 118th Cong. (2023) (written statement of testimony of Shou Chew, Chief Exec. Off., TikTok, Inc.).

We then examine the three current statutory pillars for executive authority over data flows in the name of national security. The first pillar is IEEPA, which generally grants broad authority to the President over property owned by foreign countries and their citizens. Congress, however, expressly excluded the direct or indirect regulation of "informational materials," as this Part shows. The second pillar of executive authority over data flows is the statutory basis for CFIUS, an interagency executive branch committee. This entity reviews a broad range of transactions involving foreign investments in the United States in order to protect national security. The third pillar is the TikTok Law, which orders divestiture-or-banning for this social media company while, more generally, granting the President powers over "foreign adversary controlled applications." The last section of Part I reveals the dizzying range of executive orders and regulations issued under the initial two statutory frameworks. These measures assert broad presidential powers over cross-border data flows.

A. *The TikTok Challenge: High Noon on Capitol Hill*

A quarter century after American companies became the chief means of communication for much of the world, the United States found itself for the first time confronted by Americans' widespread use of a wildly popular app owned by a company based in China. TikTok is a U.S. company owned by a company headquartered in Beijing; its app is now used by over 170 million people in the United States.[22] Thus, when TikTok's CEO first appeared before Congress on March 23, 2023,[23] members of Congress were highly engaged in the proceeding.

Billed as a hearing on "TikTok and Data Privacy," the House Energy and Commerce hearing ran nearly six hours, with members of Congress alternating between interrogating, denouncing, and berating Shou Chew, the CEO of TikTok.[24] As one representative told Chew, TikTok had accomplished what nobody, with the "exception of maybe Vladmir Putin," had done during the last three to four years: uniting a divided Congress in bipartisan agreement about its profound threat to Americans.[25]

---

22 TikTok, Inc. v. Trump, 507 F. Supp. 3d 92, 98-99 (D.D.C. 2020); Petition for Review of Constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act at 7, Tiktok Inc. v. Garland, No. 24-1113 (D.C. Cir. May 7, 2024).

23 TikTok's Chief Operating Officer, Vanessa Pappas, had previously faced another grilling before Congress in September 2022. David McCabe, *Lawmakers Grill TikTok Executive About Ties to China*, N.Y. TIMES (Sept. 14, 2022), https://www.nytimes.com/2022/09/14/technology/tiktok-china-senate.html [https://perma.cc/4X3B-DCU2].

24 *See* Justin Hendrix, *Transcript: TikTok CEO Testifies to Congress*, TECH POL'Y PRESS (Mar. 24, 2023), https://www.techpolicy.press/transcript-tiktok-ceo-testifies-to-congress [https://perma.cc/969W-8M6G].

25 *See id*.

Beyond that, the hearing demonstrated that House members were highly concerned about two threats from TikTok at the intersection of national security and data privacy.[26] The issues that centered around personal data were, first, how TikTok permitted the Chinese government to distribute targeted propaganda in the United States, and, second, how it collected personal data to spy on Americans.[27] Both dangers involve national security and data privacy.[28]

Many members of Congress declared TikTok a conduit for Communist propaganda and disinformation. Committee Chair Cathy McMorris Rodgers argued in the hearing that TikTok permitted "foreign influence in American life."[29] She added, "[I]t's like allowing the Soviet Union the power to produce Saturday morning cartoons during the Cold War, but much more powerful and much more dangerous."[30] Without citing evidence, Representative Buddy Carter claimed, "[T]he Chinese Communist Party is engaged in psychological warfare through TikTok to deliberately influence [U.S.] children."[31] This concern is shared outside of Washington. In April 2023, during the deliberations before passing a statewide ban on TikTok, a Montana legislator

26 To be sure, the congresspersons aired other concerns, but those were ones likely to be more or less the same for American-owned digital media platforms. The more generic concerns were about the addictive nature of the TikTok platform and worries that it could exacerbate mental health issues. *See id*.

27 *See id*.

28 One mechanism for surveillance might be the insertion of malicious code in the software. Christopher Wray, the Director of the Federal Bureau of Investigation, has described the possibility of the Chinese government using TikTok to plant software "on millions of devices, which gives it opportunity to potentially technically compromise personal devices." Lauren Feiner, *FBI is 'Extremely Concerned' About China's Influence Through TikTok on U.S. Users*, CNBC (Nov. 15, 2022, 3:30 PM), https://www.cnbc.com/2022/11/15/fbi-is-extremely-concerned-about-chinas-influence-through-tiktok.html [https://perma.cc/S4FY-92YB]. App stores seek to remove malware from their stores. *See, e.g.*, APPLE, BUILDING A TRUSTED ECOSYSTEM FOR MILLIONS OF APPS: A THREAT ANALYSIS OF SIDELOADING 6 (2021), https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf [https://perma.cc/L2WT-CE29] ("Supporting [the distribution of apps outside of the App Store] would cripple the privacy and security protections of the iOS platform . . . ."); *cf.* EUR. NETWORK & INFO. SEC. AGENCY, APPSTORE SECURITY: 5 LINES OF DEFENCE AGAINST MALWARE 3 (2011) (describing five methods to protect end-users from malware). TikTok's Project Texas seeks to protect against malware infiltration through code reviews by Oracle and other parties. *See* Matt Perault & Samm Sacks, *Project Texas: The Details of TikTok's Plan to Remain Operational in the United States*, LAWFARE (Jan. 26, 2023, 8:01 AM), https://www.lawfaremedia.org/article/project-texas-the-details-of-tiktok-s-plan-to-remain-operational-in-the-united-states [https://perma.cc/YUB7-TGXP] (describing how "Oracle will be responsible for identifying malicious code").

29 Hendrix, *supra* note 24.

30 *Id*.

31 *Id*.

wondered whether "TikTok is the music played by the Pied Piper to steal this generation's heart and mind."[32]

Before the digital age, foreign propaganda did not generally implicate information privacy.[33] But with their ability to combine personal data and algorithmic learning, digital platforms can draw on personal data to drive individualized content to viewers. This concern was more implicit than explicit at the House hearing, though sometimes the propaganda and privacy concerns were linked. Representative Yvette Clarke encapsulated this concern by arguing that "foreign adversaries[] [h]aving direct access to Americans' data as well as the ability to influence this content[] American[s] see on a prolific social media platform, represents an unprecedented threat to American security and to our democracy."[34]

The second major concern expressed at the hearing was about data privacy and the ability of the Chinese government to obtain access to personal information about Americans. A key concern was the 2018 Chinese National Intelligence Law, which requires organizations and citizens to "support, assist, and cooperate with national intelligence efforts in accordance with law."[35] Representative John Joyce summed up this concern: "TikTok is the spy in Americans' pockets."[36] The possibility of TikTok being used for surveillance is heightened by past cyber-intrusions often ascribed to Chinese government-related actors. The 2013-2014 hack of the U.S. government's Office of Personnel Management, where hackers gained access to the records of over twenty-one million people, has often been attributed to Chinese actors, though the U.S. government itself has not made this accusation.[37]

Many members of Congress seemed to treat the collection of personal information in the United States by a Chinese-owned entity as tantamount to a transfer of that information to the Chinese government. Similar data collection by an American-owned entity, such as Amazon, Meta, or Microsoft, has not set off the same national security alarm bells. In addition, in the case of TikTok, the concern at the hearing went beyond the privacy of individuals. Rather than viewing privacy purely as a personal interest, the policy concern

---

32 David McCabe, *A Plan to Ban TikTok in Montana Is a Preview for the Rest of the Country*, N.Y. TIMES (Apr. 12, 2023), https://www.nytimes.com/2023/04/12/technology/tiktok-ban-montana.html (quoting Rep. Neil Duram).

33 *But cf.* Lamont v. Postmaster Gen., 381 U.S. 301, 307 (1965) (deeming unconstitutional a congressional register of individuals receiving communist material from abroad).

34 Hendrix, *supra* note 24.

35 Jeremy Daum, *What China's National Intelligence Law Says, and Why It Doesn't Matter*, CHINA TRANSLATE (Feb. 22, 2024), https://www.chinalawtranslate.com/en/what-the-national-intelligence-law-says-and-why-it-doesnt-matter [https://perma.cc/6HLF-HRZT].

36 Hendrix, *supra* note 24.

37 *See* Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 548-49 (2020) (discussing the hack).

was with privacy as a *group interest*—one involving national security. For example, Representative Dan Crenshaw warned American teenagers, "You may not care that your data's being accessed now, but it will be one day when you do care about it. And here's the real problem[:] with data comes power."[38] The perceived need is to stop data collection that will transform the United States into a country whose masses are subject to blackmail and manipulation.

Through its "Project Texas," TikTok had hoped to stave off expulsion from the United States or its compelled sale.[39] This initiative, now in progress, stores data collected within the United States in data centers on American soil, discontinues access to that data by ByteDance employees in China, and modifies TikTok's corporate governance over personal data and its recommendation algorithm.[40] Under Project Texas, Oracle, a U.S. company, maintains TikTok's U.S. user data and monitors changes to TikTok's source code and algorithm.[41] Regarding governance, TikTok has created a special purpose subsidiary, called TikTok U.S. Data Security (TikTok USDS) that will manage all business functions relating to personal data.[42] An independent board of directors, with each director approved by the U.S. government, will oversee TikTok USDS with the explicit goal of safeguarding the app in the U.S. to ensure that it is free from foreign manipulation.[43] TikTok reports that it has spent $2 billion implementing this initiative.[44]

Yet, the elaborate controls of Project Texas failed to convince Congress that the app had been made safe for Americans. In enacting the TikTok Law, Congress required ByteDance, the Chinese-based company that owns TikTok, to divest itself of this platform or face being banned 270 days after the law's passage.[45] This statute makes it unlawful for an app store to offer, or a hosting service to host, "a foreign adversary controlled application" in the United States.[46] We discuss the TikTok Law below, but first turn to IEEPA,

---

38 Hendrix, *supra* note 24.

39 *About Project Texas*, TIKTOK U.S. DATA SEC., https://usds.tiktok.com/usds-about [https://perma.cc/FU8A-DBC4] (last visited Apr. 3, 2024).

40 *Id.*

41 *See* Perault & Sacks, *supra* note 28 ("Oracle Cloud will host the TikTok platform in the United States, including the algorithm and the content moderation functions.").

42 *Id.*

43 *Id.*

44 *See Petition for Review* of Constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act at 29, Tiktok Inc. v. Garland, No. 24-1113 (D.C. Cir. May 7, 2024).

45 Sapna Maheshwari & David McCabe, *Congress Passed a Bill That Could Ban TikTok. Now Comes the Hard Part.*, N.Y. TIMES (Apr. 23, 2024), https://www.nytimes.com/2024/04/23/technology/bytedance-tiktok-ban-bill.html [https://perma.cc/82CV-KD4M].

46 *See generally* 21st Century Peace Through Strength Act, H.R. 8038, 118th Cong. div. D (2024).

the second pillar of the President's authority over international flows of personal data granted in the name of national security.

B. *IEEPA and Personal Data*

The central statute empowering the executive to respond to peacetime economic emergencies is the International Emergency Economic Powers Act (IEEPA) of 1977.[47] This law was enacted during an era of congressional efforts to rein in executive power. IEEPA reflected Congress's belief that the Trading with the Enemy Act (TWEA)—a statute passed in the wake of U.S. entry into World War I—granted the President excessive discretion.[48] The 1976 congressional report that would lead to IEEPA began as follows: "A majority of Americans alive today have lived their entire lives under emergency rule."[49]

This quotation alludes to a triggering condition for the executive branch's use of its IEEPA authority, which is a formal declaration of an "emergency."[50] As of January 2024, Presidents have declared seventy national emergencies that invoke IEEPA.[51] Indeed, thirty-nine of these emergencies are ongoing.[52] The 1976 congressional report's worry about emergency rule becoming routinized is more than justified nearly fifty years later.

IEEPA has proven central to the executive branch's response to foreign companies gaining access to the personal data of Americans and to American information and communication technology. It is the principal authority under which Presidents Trump and Biden have issued executive orders regarding information and communication technology.[53] These general orders seek to safeguard the information technology used in the United States. Yet, ultimately, this statute has a notable weakness for this task: its

---

47 50 U.S.C. §§ 1701–07.

48 *See* CHRISTOPHER A. CASEY, DIANNE E. RENNACK & JENNIFER K. ELSEA, CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE 2-8 (2024) (describing the history of IEEPA); Note, *The International Emergency Economic Powers Act: A Congressional Attempt to Control Presidential Emergency Power*, 96 HARV. L. REV. 1102, 1104-10 (1983) (same).

49 SPECIAL COMM. NAT'L EMERGENCIES & DELEGATED EMERGENCY POWERS, NATIONAL EMERGENCIES AND DELEGATED EMERGENCY POWERS, S. Rep. No. 94-922, at 1 (1976).

50 50 U.S.C. § 1701(a).

51 CASEY, RENNACK & ELSEA, supra note 48, at 16.

52 *See id.* (noting that there are forty-two ongoing emergencies, all but three of which invoke IEEPA).

53 *See, e.g.*, Exec. Order No. 13,984, 86 Fed. Reg. 6837, 6837 (Jan. 25, 2021) (addressing "significant malicious cyber-enabled activities"); Exec. Order No. 14,105, 88 Fed. Reg. 54867, 54867 (Aug. 11, 2023) (addressing U.S. investments in national security technologies in countries of concern).

exemption of "informational materials." This section will explore this aspect of IEEPA and its meaning for cross-border flows of personal data.

1. The Road to the "Informational Materials" Exclusion

IEEPA is an outgrowth of TWEA, which was enacted in 1917, six months after the United States' entry into World War II.[54] During the Great Depression and then again upon the United States' entry into World War II, President Franklin Roosevelt made significant use of TWEA's grant of power. As Kathleen Claussen summarizes, TWEA was "used from the 1930s through the 1960s as a tool for monetary policy and to implement sanctions on foreign adversaries both during and outside of wartime."[55]

Sixty years later, in 1977, Congress enacted IEEPA. It did so as a two-step strategy to remake TWEA. Its first step was to reform TWEA itself; among these changes was to limit this statute solely to wartime periods.[56] As for its second reform, Congress enacted IEEPA to regulate the President's power during peacetime national emergencies. Yet, despite congressional rhetoric at the time about the need to limit the executive branch, IEEPA still offers a broad delegation of authority to the President. Once the President declares an emergency in an executive order, the resulting powers are wide reaching, allowing the President to block, regulate, prevent, or prohibit

> any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property . . . .[57]

Under IEEPA, then, the President can not only ban a foreign investment but also prevent U.S. companies from transacting with that target company. IEEPA responds to a broad concern about threats to national security caused by foreign involvement in the U.S. economy and, in response, gives the President sweeping powers.

---

54 *See* CASEY, RENNACK & ELSEA, *supra* note 48, at 2-3.

55 Kathleen Claussen, *Trade's Security Exceptionalism*, 72 STAN. L. REV. 1097, 1118 (2020).

56 As one of the sponsors of IEEPA, Representative Jonathan B. Bingham worried that TWEA gave the President nearly "dictatorial" powers. Congress was highly concerned that TWEA was being used excessively during peacetime. The last straw in that regard was President Richard Nixon drawing on TWEA in 1971 to place a ten percent tariff on all goods entering the United States. President Nixon took this action after the United States went off the gold standard. *See* CASEY, RENNACK & ELSEA, *supra* note 48, at 6-7 ("[F]ollowing U.S. military involvement in Vietnam, revelations of domestic spying, assassinations of foreign political leaders, the Watergate break-in, and other related abuses of power, Congress increasingly focused on checking the executive branch.").

57 50 U.S.C. § 1702(a)(1)(B).

IEEPA also goes beyond an interest in foreign investment in the United States to reach virtually all economic situations involving the United States that constitute "peacetime crises." An IEEPA executive order can be triggered by a threat to national security, foreign policy, or the economy.[58] Use of IEEPA by the President begins with an executive order declaring a national emergency with respect to "any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States."[59] Such an order can authorize federal agencies to "designate" foreign persons by placing them on a list maintained by the Office of Foreign Assets Control (OFAC). This step can mean forbidding "virtually any economic interaction with a designated person."[60]

2. Ensuring Free Trade in Ideas: The Berman Amendment and Free Trade in Ideas Act

As originally enacted, IEEPA did not grant peacetime emergency power over a "personal communication."[61] Free speech was to be maintained for foreign powers and foreign persons, even if the President believed that it might undermine national security, foreign policy, or the U.S. economy. But IEEPA also contained an exception to this restriction concerning "a transfer of anything of value."[62] The statute originally declared that "[t]he authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly . . . any postal, telegraphic, telephonic or other personal communication, which does not involve a transfer of anything of value."[63] Thus, IEEPA first strips power from the President by providing an exception to IEEPA's broad grant of authority over an extensive list of communications, which the President cannot regulate under IEEPA. But, through its exception to this exception, concerning "the transfer of anything of value," IEEPA assigns significant regulatory power back to the Executive. The general idea is that while the international flow of

58 *Id.* § 1701(a).

59 *Id.*

60 Open Soc'y Just. Initiative v. Trump, 510 F. Supp. 3d 198, 203 (S.D.N.Y. 2021). Violating an order issued under IEEPA can lead to a civil penalty of up to twice the value of the blocked transaction. A willful violation of an IEEPA order is also subject to criminal fines and up to twenty years' imprisonment. The process of being made subject to the enforcement of IEEPA's civil and criminal penalties is separate from the initial OFAC designation of being a "sanctioned person." *Id.* at 23-24; *see* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2201 (2021) (describing how TransUnion packaged and sold a database of OFAC designations to its business customers).

61 CASEY, RENNACK & ELSEA, *supra* note 48, at 12.

62 *Id.*

63 50 U.S.C. § 1702(b)(1).

personal communications will be outside the powers of the Presidency, things of value, like a wiring of funds, can be regulated and restricted.

Within a decade of IEEPA's enactment, however, this approach did not seem adequate to protect information transmissions. American publishers and others became alarmed that offering works from authors living in IEEPA-sanctioned countries might violate the law. Such a publication would arguably not be a "personal communication," but might be something "of value." For example, IEEPA might have allowed the President to stop a U.S. publisher from selling printed matter from Warsaw Pact nations.[64] These concerns led Congress to enact two successive amendments to IEEPA—the first in 1988, and the second in 1994. Both were sponsored by Representative Howard Berman. For clarity's sake, we will refer to the first amendment as the "Berman Amendment" and the second amendment as the "Free Trade in Ideas Act," as it was also termed.

Through the 1988 enactment of the Berman Amendment, Congress explicitly excluded the cross-border transfer of "informational materials" from IEEPA's grant of authority to the President.[65] The amendment listed a wide range of material that it sought to protect. Pursuant to the Berman Amendment, the President lacks authority under IEEPA to regulate "the importation from any country, or the exportation to any country, whether commercial or otherwise, of publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, or other informational materials."[66] The "informational materials" exception thus protects a two-sided flow of information across borders through its coverage of both the "importation from any country" and the "exportation to any country" of informational materials.[67]

The list of technologies in the Berman Amendment is open-ended; its enumerated list ends by referencing its extension to "other informational materials."[68] Nonetheless, the entity charged with enforcing sanctions, OFAC, took a restrictive view of what constituted "informational materials," excluding "intangible items, such as telecommunications transmissions."[69] In response to this OFAC action, Representative Howard Berman introduced a

---

64 *Cf.* Toni Feder, *US Government Backs Off from Imposing Restrictions on Publishers*, PHYSICS TODAY, May 2004, at 28, https://pubs.aip.org/physicstoday/article/57/5/28/412551/US-Government-Backs-Off-From-Imposing-Restrictions [https://perma.cc/T9CY-BVY6] (describing the Institute of Electrical and Electronics Engineers' concern that their payment for a conference venue in Tehran would have violated IEEPA).

65 Berman Amendment, Pub. L. No. 100-418, § 2502(b)(C)(3), 102 Stat. 1371 (1988).

66 *Id.*

67 *Id.*

68 *Id.*

69 *See* Foreign Assets Control Regulations and Cuban Assets Control Regulations, 54 Fed. Reg. 5229, 5231 (Feb. 2, 1989).

further revision to IEEPA.[70] In 1994, Congress enacted Berman's second amendment to IEEPA, the Free Trade in Ideas Act.[71]

This later revision of IEEPA excluded control over transactions concerning informational materials "regardless of format or medium of transmission."[72] Congress also added new items to the law's nonexclusive litany of enumerated media that qualified as "informational materials." The newly protected objects were "compact disks, CD ROMs, artworks, and news wire feeds."[73]

The result of these amendments proves significant for today's digital platforms like TikTok. To be sure, IEEPA's original exception for any "personal communication" and its later exception for "informational materials" were crafted during the Cold War and before today's digital age. Nevertheless, these amendments were made with deep awareness of the risk of foreign disinformation campaigns. In response to those who worried about communist influence, Representative Berman declared, "[W]e fear no outside ideas."[74] He made clear that U.S. "confiden[ce] in the superiority of [its] national values" supported free trade in ideas.[75] Arguing in favor of what would be the 1988 amendment and the first information flow amendment to IEEPA, Senator Charles Mathias embraced "open and robust debate in the marketplace of ideas."[76] To promote "free trade in ideas," Mathias quoted Justice Oliver Wendell Holmes Jr.'s famous aphorism: "[T]he best test of truth is the power of thought to get itself accepted in the competition of the market."[77]

This policy perspective was also reflected in the academic literature of the time. For example, Burt Neuborne and Steven R. Shapiro recognized in 1985 that "a calculated 'disinformation' campaign orchestrated by a hostile national" could "undermine American foreign policy."[78] But Neuborne and Shapiro argued that using this risk to prohibit the free flow of information

---

70 Representative Berman first introduced this revision in 1989. *See* The Free Trade in Ideas Act of 1989, H.R. 1767, 101st Cong. (1989).

71 *See* Free Trade in Ideas Act, Pub. L. No. 103-236, § 525, 108 Stat. 474 (1994) (codified as amended at 50 U.S.C. § 1702(b)(3)).

72 *Id.* § 525(b).

73 *Id.*

74 *Free Trade in Ideas Act of 1992: Joint Hearing on H.R. 5406 Before the Subcomms. on Int'l Econ. Pol'y & Trade and Int'l Operations of the Comm. on Foreign Affs.*, 102d Cong. 5 (1992) (opening statement of Howard L. Berman, Chairman, Subcomm. On Int'l Operations).

75 *Id.*

76 132 CONG. REC. 6550-51 (1986) (statement of Senator Charles Mathias).

77 *Id.* at 6550.

78 Burt Neuborne & Steven R. Shapiro, *The Nylon Curtain: America's National Border and the Free Flow of Ideas*, 26 WM. & MARY L. REV. 719, 768-69 (1985).

was "difficult to accept in a system based on the premise that the answer to allegedly false speech is more speech, not suppression."[79]

IEEPA is today more important than ever. It provided the statutory basis for the Trump administration's attempts to ban TikTok and other Chinese-owned apps. It also provides the foundation for the Biden administration's 2024 executive order, discussed in the introduction, to restrict sales by data brokers of the sensitive personal data of Americans to entities in so-called "countries of concern."[80] We return to the Trump ban and the Biden 2024 executive order below.[81]

C. *CFIUS and Personal Data*

In its March 2023 hearings, when the House Committee mentioned the laws giving the United States authority over TikTok, it most frequently referenced the CFIUS framework.[82] Initially established in 1975 by President Ford's executive order, and later solidified through the 1988 Exon-Florio Amendment to a Defense Department appropriation bill, CFIUS is an interagency committee within the executive branch.[83] Chaired by the Treasury Secretary, CFIUS reviews any "covered transaction"—a term which refers to "[a]ny merger, acquisition, or takeover" involving "foreign control" of a wide range of U.S. businesses.[84] In turn, regulators have interpreted "control" broadly. As one account explains, "even minority voting interests in the range of ten percent may be deemed controlling, especially when combined with other rights or relationships between the parties."[85] Through this Committee, Congress grants the President power to review business transactions that will harm national security. CFIUS legislation aims to prevent foreign entities from gaining access to certain kinds of assets; its touchstone is whether an investment transaction poses a national security risk.

Over time, the role of CFIUS has changed. In 2009, David Zaring characterized CFIUS as a mere "congressional notification service."[86] He pointed to a "mildness of the executive role" under it and observed that the "connection between CFIUS activity and congressional oversight is now

---

79 *Id.* at 769.

80 *See supra* note 13 and accompanying text.

81 *See infra* Section I.D.

82 *See, e.g.*, Hendrix, *supra* note 24 (statement of Representative Kelly Armstrong).

83 JAMES K. JACKSON, CONG. RSCH. SERV., RL33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) 5-8 (2020).

84 50 U.S.C. § 4565(a)(4).

85 Jonathan Wakely & Andrew Indorf, *Managing National Security Risk in an Open Economy: Reforming the Committee of Foreign Investment in the United States*, 9 HARV. NAT'L SEC. J. 1, 7-8 (2018).

86 David Zaring, *CFIUS as a Congressional Notification Service*, 83 S. CAL. L. REV. 81, 83 (2009).

extremely close."[87] Today, CFIUS is a prime example of the congressional expansion of presidential power and embodies a phenomenon that Kristen Eichensehr and Cathy Hwang call "national security creep" over corporate transactions.[88] As Eichensehr and Hwang explain, the executive branch now makes increasingly broad claims about the impact of corporate dealmaking on national security and thus reviews, renegotiates, and sometimes blocks corporate transactions.[89] CFIUS review, they argue, has taken on a "tentacular" nature, where a foreign party seeking investment in the United States is swept up in a battle with the arms of a Congress-enabled, executive branch octopus.[90]

The most important recent expansion of CFIUS power occurred in 2018, when Congress promulgated the Foreign Investment Risk Review Modernization Act ("FIRRMA"). For the first time, FIRRMA explicitly included personal data as one of the covered assets subject to CFIUS review.[91] FIRRMA extends CFIUS scrutiny to any controlling or non-controlling investment that permits a foreign person access to so-called "sensitive personal data of [U.S.] citizens that may be exploited in a manner that threatens national security."[92] It is not necessary that the foreign entity be seeking control of the U.S. entity: this review reaches non-controlling investments by a foreign party in a U.S. business that will include "[a]ny involvement . . . in substantive decision-making of the [U.S.] business regarding: the use, development, acquisition, safekeeping, or release of sensitive personal data of [U.S.] citizens maintained or collected by the [U.S.] business."[93] For TikTok, the CFIUS process became applicable once ByteDance, a company based in China, acquired the U.S. company Musical.ly in 2017.[94]

CFIUS has utilized a wide range of mitigation measures for any national security risks that it identifies, including divestiture of assets or operations, forfeiture of sensitive contracts, appointment of special compliance personnel, restriction of operations to insulate sensitive operations from foreign control, or appointment of a proxy board consisting of U.S. persons.[95]

---

87 *Id.* at 81, 97.

88 Kristen E. Eichensehr & Cathy Hwang, *National Security Creep in Corporate Transactions*, 123 COLUM. L. REV. 549, 551 (2023).

89 *Id.* at 562-70 (detailing CFIUS's increasing scope).

90 *Id.* at 566.

91 PRAC. L. CORP. & SEC., *supra* note 20, at 2-3.

92 *Id.* at 3.

93 *Id.*

94 *See* Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51297, 51297 (Aug. 14, 2020) (ordering ByteDance to divest after its merger with Musical.ly).

95 *See* BAKER BOTTS, A GUIDE TO DEMYSTIFY THE CFIUS PROCESS 7 ("There are many variations of mitigation agreements such as implementation of security plans, periodic compliance

A Chinese company's 2019 forced sale of Grindr, a dating app, was due to a CFIUS decision.[96] TikTok's Project Texas also borrows from this toolset—as noted in Section I.A., it would have relied on special compliance personnel and an independent board overseeing TikTok USDS.

In enacting FIRRMA, Congress recognized a new reality of the twenty-first century, which is the centrality of personal data to national prosperity and national security. To be sure, FIRRMA acknowledges the "substantial economic benefits to the United States" of foreign investment.[97] At the same time, it calls for CFIUS scrutiny of "the extent to which a covered transaction is likely to expose, either directly or indirectly, personally identifiable information, genetic information, or other sensitive data of United States citizens to access by a foreign government or foreign person that may exploit that information in a manner that threatens national security."[98] Therein lies the national securitization of personal data. Yet, as the Congressional Research Service notes, how the Committee is "to evaluate the national security implications of . . . personally identifiable information" remains an open question.[99]

D. *The TikTok Law and Personal Data*

Considerably augmenting presidential power over international flows of personal data, Congress enacted the Protecting Americans from Foreign Adversary Controlled Applications Act in April 2024, going from introduction in the House in March to passage and signing at remarkable speed.[100] Because the law unusually targets a particular company, TikTok, and its parent, ByteDance, for sanctions, we refer to it here as simply the "TikTok

audits and certifications, proxy boards made up only of U.S. citizens, or even restructuring of the transaction to hive off a business that CFIUS does not want the foreign party to have any access or control over.").

96 *See* Carl O'Donnell, Liana B. Baker & Echo Wang, *Exclusive: Told U.S. Security at Risk, Chinese Firm Seeks to Sell Grindr Dating App*, REUTERS (Mar. 27, 2019, 3:50 PM), https://www.reuters.com/article/us-grindr-m-a-exclusive/exclusive-u-s-pushes-chinese-owner-of-grindr-to-divest-the-dating-app-sources-idUSKCN1R809L.

97 Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1702(b)(1), 132 Stat. 2177 (2018).

98 *Id.* § 1702(c)(5).

99 JACKSON, *supra* note 83, at 40.

100 We reserve the discussion of another statute targeting data flows through data brokers, passed as part of the TikTok Law package, for the following Section, where we also discuss an executive order targeting the same activity. *See infra* notes 158-170 and accompanying text.

Law."[101] However, the law also sweeps in other companies, as we will now explore.

The path to enactment of the TikTok Law after the high-profile House hearing in March 2023, discussed above,[102] was far from preordained. As the *New York Times* explained, post-hearing activity involved "a tiny group of lawmakers . . . plotting a secretive effort" that included input from the Justice Department and the White House, and then "a race to the president's desk" within seven weeks of the public introduction of the bill by Congressmen Mike Gallagher and Raja Krishnamoorthi, Chair and Ranking Member, respectively, of the House Select Committee on the Chinese Communist Party.[103] Congressman Gallagher explained that his principal concern was the possibility of China's possible use of the app for "propaganda."[104] Some in Congress worried that TikTok was already spreading Chinese propaganda by preferencing certain content over others.[105]

The House passed the TikTok bill twice, first as a stand-alone bill, and then again as part of an omnibus package with a slight revision.[106] The one

---

101 *See* 21st Century Peace Through Strength Act, H.R. 8038, 118th Cong. div. D § 2(g)(3) (2024) (defining "foreign adversary controlled application" to include applications and websites of ByteDance, TikTok, and their subsidiaries). An early draft of the law posted online, titled "TIKTOK.XML," made the focus clear. *See* Drew Harwell, *TikTok and the U.S. Government Dig in for a Legal War over Potential Ban,* WASH. POST (Apr. 25, 2024, 6:00 AM), https://www.washingtonpost.com/technology/2024/04/25/tiktok-legal-battle-is-certain [https://perma.cc/E4MA-7ACK].

102 *See supra* Section I.A.

103 *See* Sapna Maheshwari, David McCabe & Cecilia Kang, *'Thunder Run': Behind Lawmakers' Secretive Push to Pass the TikTok Bill*, N.Y. TIMES (Apr. 24, 2024), https://www.nytimes.com/2024/04/24/technology/tiktok-ban-congress.html [https://perma.cc/W3FJ-TL9L].

104 *See* Jane Coaston, *What the TikTok Bill Is Really About, According to a Leading Republican*, N.Y. TIMES (Apr. 1, 2024), https://www.nytimes.com/2024/04/01/opinion/mike-gallagher-tiktok-sale-ban.html [https://perma.cc/SD5R-GGZ8].

105 *See* Stu Woo, Georgia Wells & Raffaele Huang, *How TikTok Was Blindsided by U.S. Bill That Could Ban It*, WALL ST. J. (Mar. 12, 2024, 3:42 PM), https://www.wsj.com/tech/how-tiktok-was-blindsided-by-a-u-s-bill-that-could-ban-it-7201ac8b [https://perma.cc/686W-Z2RP] ("[Congressman Mike] Gallagher heads a House committee focused on China, and the concerns about Israel-Hamas videos on TikTok spurred him and other committee members to renew their attempts to force a sale or ban."); David Leonhardt, *TikTok's Pro-China Tilt*, N.Y TIMES (Apr. 24, 2024), https://www.nytimes.com/2024/04/24/briefing/tiktok-ban-bill-congress.html ("Already, there is evidence that China uses TikTok as a propaganda tool."). For an argument that the cited evidence of the alleged tilt with respect to subjects sensitive to China's interests is based on faulty analysis, see Paul Matzko, *When You Can't Believe Your Eyes*, SUBSTACK (Apr. 15, 2024), https://matzko.substack.com/p/when-you-cant-believe-your-eyes?r=k5clf&utm_medium=ios&triedRedirect=true [https://perma.cc/F83G-9YED].

106 *See* Protecting Americans from Foreign Adversary Controlled Applications Act, H.R. 7521, 118th Cong. (2024) (passed by the House on March 13, 2024); 21st Century Peace Through Strength Act, H.R. 8038, 118th Cong. div. D (2024) (passed by the House on April 20, 2024). The Senate passed the package on April 23, 2024, and the President signed it into law the next day. *See* Maheshwari, McCabe & Kang, *supra* note 103.

revision to the text was to extend the deadline for divestiture from 180 to 270 days.[107] By folding this statute into a larger bill, its path was eased through the Senate, where it was considered as a single package.[108] The larger bill in question, among other matters, contained military aid for Ukraine, Israel, and Taiwan, and placed sanctions on Iran and on transnational criminal organizations engaged in international trafficking of fentanyl.[109]

The House passed the final version of the TikTok bill as part of the 21st Century Peace through Strength Act by a vote of 360 to 58, and the Senate passed the omnibus bill by a vote of 79 to 18.[110] Having supported the bill and the larger military aid package throughout the legislative process, President Biden signed the bill, including the TikTok Law, promptly upon its presentment to the White House on April 24, 2024. This action started the countdown for TikTok's sale or ban.[111] President Biden's reelection campaign, which had just joined the app in February 2024, then announced that it would continue to use the app, despite the President's assertions that the app posed a national security threat under its current ownership.[112] Any sale or ban would likely occur after the November 2024 election, with the statute's 270 date divestiture deadline occurring on January 19, 2025, the day before the presidential inauguration.

The TikTok Law prohibits any company from distributing, maintaining, or hosting any app or website that is identified as a "foreign adversary controlled application."[113] The statute provides two ways to earn this designation: first, it covers all applications offered by ByteDance, TikTok, or any of their successors or subsidiaries, and second, it extends to any application offering user-generated content with at least a million monthly users that is operated by a company headquartered in an identified adversary

---

107 H.R. 8038 § 2(a)(2).

108 Georgia Wells & Kristina Peterson, *How TikTok Lost the War in Washington*, WALL ST. J. (Apr. 28, 2024, 5:30 AM), https://www.wsj.com/tech/how-tiktok-lost-the-war-in-washington-bbc419cc?mod=Searchresults_pos4&page=1 (noting that the bill's proponents attached it to "a must pass bill," "a Senate-backed $95 billion foreign aid package to Ukraine and Israel," in order to obtain passage in the Senate).

109 *See* H.R. 815, 118th Cong. (2024) (including 18 different acts).

110 *See All Actions: H.R. 8038–118th Congress (2023-2024)*, CONGRESS.GOV, https://www.congress.gov/bill/118th-congress/house-bill/8038/all-actions (last visited Apr. 30, 2024); *All Actions: H.R. 815–118th Congress (2023-2024)*, CONGRESS.GOV, https://www.congress.gov/bill/118th-congress/house-bill/815/all-actions (last visited Apr. 30, 2024).

111 *See* Zolan Kanno-Youngs, *Biden Says Weapons Will Flow to Ukraine Within Hours as He Signs Aid Bill*, N.Y. TIMES (Apr. 24, 2024), https://www.nytimes.com/2024/04/24/us/politics/biden-ukraine-israel-aid.html.

112 Demetri Sevastopulo, *Biden Campaign Will Continue to Use TikTok Despite Divest-or-Ban Law*, FIN. TIMES (Apr. 24, 2024), https://www.ft.com/content/fdf5ddac-36a2-4bc1-bc46-051aabbc38a0 [https://perma.cc/YE7W-E3M5].

113 21st Century Peace Through Strength Act, H.R. 8038, 118th Cong. div. D § 2(a)(1) (2024).

country and designated by the President as "a significant threat to the national security of the United States."[114] The statute provides the identified application with an alternative to a ban—transfer of ownership to a company that is not from one of the adversary nations.[115]

Before the President can designate an app other than TikTok and its sister apps, the President must provide public notice of the planned designation and a public report to Congress "describing the specific national security concern involved and containing a classified annex and a description of what assets would need to be divested to execute a qualified divestiture."[116] The TikTok Law borrows an existing definition of "foreign adversary" from a statute barring transactions in specialty metals with possible military uses.[117] That existing law names China, North Korea, Russia, and Iran as adversaries. It does so to bar the purchase or sale of these specialty metals to or from these adversary countries. Where we once blocked trade with these foreign countries with respect to certain metals that might have military uses, we now bar those countries from offering popular media services.

The TikTok Law thus offers a stark choice for TikTok and, in the future, for any designated foreign adversary controlled application—either divest or cease functioning in the United States. If the company will not or cannot sell its application to buyers from countries other than the adversary countries, its applications would lose access to app stores necessary for users to download or update the app in the United States, and to any hosting service in the United States, all of which would be tantamount to a United States ban. By way of context, app divestiture orders are not entirely new. CFIUS ordered a Chinese company to sell Grindr, the dating app, in March 2019, which the Chinese company did in May 2020.[118] The Chinese owner did not challenge the ban in court, so its legality was never tested. The TikTok Law also permits the Attorney General to seek weighty penalties of up to $5,000

---

114 *Id.* §§ 2(g)(2)–(3) (defining "covered company" as a company that permits users to share content with more than a million monthly active users).

115 *Id.* § 2(c). The statute permits the President to provide an additional 90 day reprieve to effectuate the sale, thus potentially extending the period to sell to a total of 360 days. *See id.* § 2(a)(3).

116 *Id.* §§ 2(g)(3)(B)(ii)(I)–(II).

117 *See* 10 U.S.C. § 4872(d)(2).

118 *See* Jay Peters, *Grindr Has Been Sold by Its Chinese Owner After the US Expressed Security Concerns*, VERGE (Mar. 6, 2020, 1:26 PM), https://www.theverge.com/2020/3/6/21168079/grindr-sold-chinese-owner-us-cfius-security-concerns-kunlun-lgbtq [https://perma.cc/SGE6-PAGU]; Sarah Bauerle Danzman & Geoffrey Gertz, *Why is the U.S. Forcing a Chinese Company to Sell the Gay Dating App Grindr?*, WASH. POST (Apr. 3, 2019, 7:00 AM), https://www.washingtonpost.com/politics/2019/04/03/why-is-us-is-forcing-chinese-company-sell-gay-dating-app-grindr [https://perma.cc/9DCW-9BRY]; Echo Wang, *China's Kunlun Says U.S. Approves Sale of Grindr to Investor Group*, REUTERS (May 29, 2020, 1:41 PM), https://www.reuters.com/article/us-grindr-m-a-sanvincente-idUSKBN2352PR.

per user, a significant sum for an app like TikTok with more than 170 million U.S. users.

In response to this divestiture-or-ban statute, CEO Shou Zi Chew responded that TikTok wasn't "going anywhere."[119] He assured the public, "The facts and the Constitution are on our side and we expect to prevail again."[120] The chief challenge by TikTok and its users to the TikTok Law is on First Amendment grounds, and the American Civil Liberties Union (ACLU) has already declared the law to be "an unconstitutional ban in disguise."[121] Jenna Leventoff, ACLU Senior Policy Counsel, predicted, "Banning a social media platform that hundreds of millions of Americans use to express themselves would have devastating consequences for all of our First Amendment rights, and will almost certainly be struck down in court."[122]

In sum, the TikTok Law represents a third statutory pillar for the President's authority over data flows to protect national security. It enhances executive authority in significant ways. Unlike CFIUS, the executive does not need an inbound investment in order to engage in a national security review of a social media app.[123] And unlike IEEPA and the executive orders issued under it, the TikTok Law contains no statutory exclusion or carve outs of the President's power, direct or indirect, over cross-border information flows. Of course, no statute can violate constitutional protections, and it remains to be seen whether the TikTok Law will survive constitutional scrutiny, at least as applied to TikTok itself. Beyond the three statutory pillars just discussed, there are a number of important related executive orders and regulations that assert and structure the President's authority over cross-border data flows, and we now turn to this topic.

E. Executive Orders and Regulations

Over the last few years, presidents have enlarged their powers over cross-border data flows by issuing executive orders and implementing regulations.

---

119 David Shepardson, *TikTok CEO Expects to Defeat US Ban: 'We Aren't Going Anywhere'*, REUTERS (Apr. 24, 2024, 5:44 PM), https://www.reuters.com/technology/tiktok-ceo-expects-defeat-us-restrictions-we-arent-going-anywhere-2024-04-24/?taid=6629833d76e7ac0001c9b691.

120 *Id.*

121 Press Release, Am. C.L. Union, ACLU Statement on Congress' Latest Attempt to Ban TikTok and Restrict Free Speech Online (Apr. 23, 2024), https://www.aclu.org/press-releases/aclu-statement-on-congress-latest-attempt-to-ban-tiktok-and-restrict-free-speech-online [https://perma.cc/ZK3V-QVA2]; *see* Petition for Review of Constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act, Tiktok Inc. v. Garland, No. 24-1113 (D.C. Cir. May 7, 2024); Petition for Review and Complaint for Declaratory and Injunctive Relief, Firebaugh v. Garland, No. 24-1130 (D.C. Cir. May 14, 2024).

122 *Id.*

123 *See supra* Section I.C.

Executive orders are presidential directives issued pursuant to the President's Article II powers or a delegation of power from Congress.[124] Executive orders typically direct various governmental agencies in their application and enforcement of the law and can instruct agencies to issue regulations.[125] The story of presidential action regarding cross-border data flows has seen a marked evolution from the Trump to Biden administrations. When Trump was President, the executive branch focused on a few companies with Chinese ownership. During the Biden administration, attention has broadened to any foreign-owned entity with access to "sensitive data." To assist in comprehension of this shifting landscape, we include a timeline of these executive orders and rules in an appendix to this Article.[126]

On May 15, 2019, relying on IEEPA as well as his inherent powers as Executive, President Trump issued Executive Order 13873 titled "Securing the Information and Communications Technology and Services Supply Chain."[127] The order first declares a national emergency with respect to foreign adversaries exploiting vulnerabilities in the nation's information and communications technology and services.[128] The order then authorizes the Commerce Secretary, acting in consultation with other executive officers, to prohibit any transaction by a person subject to a foreign jurisdiction involving any information and communications technology or service that the Secretary determines "poses an unacceptable risk to the national security of the United States . . . ."[129]

Executive Order 13873 marked a broadening of executive branch authority. It grants the Secretary of Commerce the authority to ban the acquisition or use in the United States of a technology or service if the Secretary concludes that the technology or service threatens the "security, integrity, and reliability of information and communications technology and services provided and used in the United States."[130] Congress had already indicated a similar concern in enacting the Secure and Trusted Communications Networks Act of 2019, which focuses on communications hardware.[131] This statute authorizes the Federal Communications Commission to prohibit advanced communication services providers in the United States from purchasing listed foreign-manufactured equipment.[132] This law also provides funds for a

124 ABIGAIL A. GRABER, CONG. RSCH. SERV., R46738, EXECUTIVE ORDERS: AN INTRODUCTION 1 (2021).

125 *See, e.g.*, *id.* at 16-17 (summarizing the use of executive orders over time).

126 *See infra* Appendix A.

127 *See* Exec. Order No. 13,873, 84 Fed. Reg. 22689, 22689 (May 17, 2019).

128 *See id.*

129 *See id.* at 22689-90.

130 *Id.* at 22689.

131 *See generally* 47 U.S.C. §§ 1601-09.

132 *See id.* § 1601.

"rip and replace" program focused on hardware.[133] Under "rip and replace," regulated telecommunications providers are eligible for millions in federal funds for their costs in removing and replacing network equipment manufactured by either of two Chinese companies—Huawei Technologies Company or ZTE Corporation.[134]

Under Executive Order 13873, the executive branch sought to extend this ban on transactions involving the acquisition or use of certain technology, whether due to the technology's impact individually or "considered as a class."[135] While much of the law concerning foreign investment and national security previously focused on foreign ownership of the entity, this order and its implementing rule sweep in entities "subject to the jurisdiction or direction" of a country identified as foreign adversary.[136] This language means that even U.S. companies might drift into the purview of Executive Order 13873 should any of their operations with access to personal data of U.S. persons be located within an adversary nation.

The first actions under Executive Order 13873 came in August 2020, with the Trump administration announcing dramatic bans on TikTok and the Chinese messaging app, WeChat. These actions were taken in Executive Order 13942 (the TikTok ban) and Executive Order 13943 (the WeChat ban); these orders banned any transaction with TikTok, TikTok's parent ByteDance, or WeChat, effective forty-five days after each order's issuance date respectively.[137] These bans would have effectively shut down TikTok and WeChat in the United States had three federal courts not issued injunctions blocking the orders.[138] Another executive order issued on January 5, 2021 targeted additional Chinese apps. Executive Order 13971, "Addressing the Threat Posed By Applications and Other Software Developed or Controlled By Chinese Companies," barred transactions with companies that provide the

133 *Id.* § 1603 (referred to as the "Secure and Trusted Communications Networks Reimbursement Program"); *see* Cecilia Kang, *'Rip and Replace': The Tech Cold War Is Upending Wireless Carriers*, N.Y. TIMES (May 10, 2023), https://www.nytimes.com/2023/05/09/technology/cellular-china-us-zte-huawei.html (describing the program).

134 *See Secure and Trusted Communications Networks Reimbursement Program*, FED. COMMC'NS COMM'N (Feb. 27, 2024), https://www.fcc.gov/supplychain/reimbursement [https://perma.cc/J6P5-WBBF] (offering to reimburse advanced communications services providers for "reasonable expenses").

135 *See* Exec. Order No. 13,873, 84 Fed. Reg. 22689, 22689 (May 17, 2019).

136 *Id.* at 22689-90; Securing the Information and Communications Technology and Services Supply Chain, 15 C.F.R. § 7(a)(1) (2024).

137 *See* Exec. Order No. 13,942, 85 Fed. Reg. 48637, 48637-38 (Aug. 11, 2020), *revoked by* Exec. Order No. 14,034, 86 Fed. Reg. 31424 (June 11, 2021); Exec. Order No. 13,943, 85 Fed. Reg. 48641, 48641-42 (Aug. 11, 2020), *revoked by* Exec. Order No. 14,034, 86 Fed. Reg. at 31424.

138 For a detailed description, see generally Anupam Chander, *Trump v. Tiktok*, 55 VAND. J. TRANSNAT'L L. 5 (2022).

following Chinese apps: Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay, and WPS Office.[139]

On January 19, 2021, the final day of the Trump administration, the Commerce Department issued rules to implement Executive Order 13873.[140] The "Supply Chain Rule" identified China (including Hong Kong), Cuba, Iran, North Korea, Russia, and the Nicolás Maduro regime in Venezuela as foreign adversaries.[141] The rule also pointed to "data exfiltration" as a key concern because it might allow "a foreign adversary to track the locations of Americans, build dossiers of sensitive personal data for blackmail, and conduct corporate espionage from inside the borders of the United States."[142] Where Executive Order 13873 spoke of unspecified "vulnerabilities" and "threats" to information and communications technologies,[143] the Supply Chain Rule focused directly on personal data, including a possible international transfer of that data. Under the rule, the Commerce Secretary can block or require mitigation measures for information and communications technology or services provided by persons subject to the jurisdiction of a foreign adversary.[144]

Upon taking office, the Biden administration offered both continuity with and changes from the Trump administration in this policy area. As for continuity, it allowed the Supply Chain Rule to take effect without modification on March 22, 2021.[145] Then, on June 9, 2021, the administration began to develop its own approach to the national security risks raised by foreign platforms. First, it issued a new executive order, Executive Order 14034, on "Protecting Americans' Sensitive Data from Foreign Adversaries," withdrawing Trump's executive orders banning transactions with TikTok, WeChat, and a half-dozen other apps.[146] Second, through this new executive order, the administration indicated that it would take a broad view of how foreign-controlled applications and platforms might pose a security risk to Americans and their personal data.[147] As the title of the executive order made

---

139 *See* Exec. Order No. 13,971, 86 Fed. Reg. 1249, 1250 (Jan. 8, 2020), *revoked by* Exec. Order No. 14,034, 86 Fed. Reg. at 31424.

140 *See* Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909 (Jan. 19, 2021) (codified at 15 C.F.R. pt. 7).

141 *Id.* at 4911.

142 *Id.* at 4910.

143 *See, e.g.*, Exec. Order 13873, 84 Fed. Reg. 22689, 22689 (May 17, 2019) ("[F]oreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services . . . .").

144 Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4910 (Jan. 19, 2021) (codified at 15 C.F.R. pt. 7).

145 *See id.* at 4909; *see also* Securing the Information and Communications Technology and Services Supply Chain, 15 C.F.R. pt. 7 (2024).

146 *See* Exec. Order No. 14,034, 86 Fed. Reg. 31423, 31424 (June 11, 2021).

147 *See id.* at 31423.

clear, the turn to personal data as a key national security concern was now complete.

The Biden order requires the Secretary of Commerce to evaluate the threat of "connected software applications [] designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary."[148] Moreover, it declared that an ongoing emergency was underway due to "a variety of factors, including the continuing effort of foreign adversaries to steal or otherwise obtain United States persons' data."[149] An accompanying fact sheet from the White House singled out China as a country that "seek[s] to leverage digital technologies and Americans' data in ways that present unacceptable national security risks while advancing authoritarian controls and interests."[150] In short, the Biden administration moved from a national security strategy during the Trump era directed at just a few companies with Chinese origins to a more general approach that promises to assess "threats through rigorous, evidence-based analysis."[151] As part of this broader-based strategy, the Biden administration issued two additional executive orders—Executive Order 14083 and Executive Order 14117.

In Executive Order 14083, "Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States," issued on September 15, 2022, the Biden administration sought to refine CFIUS.[152] The order referenced two existing elements in the CFIUS statute, namely supply chain resiliency and the nation's technological leadership.[153] It instructed CFIUS to consider three additional factors in considering investment transactions: aggregate industry investment trends, cybersecurity, and U.S. persons' "sensitive data."[154] This order, however, did not use the term "sensitive *personal* data," which had been employed in Executive Order 14034 and defined in earlier CFIUS regulations interpreting FIRRMA.[155]

---

148 *See id.* at 31424.

149 *Id.*

150 Press Release, White House, Fact Sheet: Executive Order Protecting Americans' Sensitive Data from Foreign Adversaries (June 9, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data [https://perma.cc/PWC4-K2A3].

151 Exec. Order No. 14,034, 86 Fed. Reg. at 31423.

152 *See* Exec. Order No. 14,083, 87 Fed. Reg. 57369, 57369 (Sep. 20, 2022) ("[T]his order provides direction to [CFIUS] to ensure that, in reviewing transactions within its jurisdiction (covered transactions), [CFIUS's] review remains responsive to evolving national security risks.").

153 *Id.* at 57370-71.

154 *Id.* at 57371-73.

155 *Compare, e.g.*, *id. with* Exec. Order No. 14,034, 86 Fed. Reg. at 31423 *and* 31 CFR § 800.241 (2024) (defining "sensitive personal data").

This new term represents a further broadening by the Biden administration of the executive branch's perspective on data-driven threats to national security. As an example, CFIUS is instructed to consider, "as appropriate, whether a covered transaction involves a United States business that: . . . has access to data on sub-populations in the United States that could be used by a foreign person to target individuals or groups of individuals in the United States in a manner that threatens national security."[156] The executive order limits itself to "bulk" transfers, but leaves the thresholds to future rule-making by the Department of Justice, which proposes thresholds from data about 100 to 1,000,000 persons, depending on the type of data involved.[157]

Finally, the Biden administration addressed the international sale by data brokers of American's personal information through Executive Order 14117, which was issued on February 28, 2024.[158] Congress then followed this approach by enacting the Protecting Americans' Data from Foreign Adversaries Act ("PADFA") as part of the the omnibus bill also containing the TikTok Law.[159] We now discuss the executive order and PADFA as both illustrate a similar patchwork approach to foreign data flows.

Drawing on IEEPA as well as the President's constitutional authority, the executive order seeks "to restrict access by countries of concern" to certain personal data.[160] Executive Order 14117 authorizes the Department of Justice to restrict transactions involving either "bulk sensitive personal data or United States Government-related data."[161] The order defines "sensitive personal data" to include personal identifiers, geolocational data, biometric identifiers, personal health data, personal financial data, "or any combination thereof."[162] In an apparent first for a privacy-related measure, Executive Order 14117 also extends to both genomic data and "human 'omic data." The term "'omic data" is shorthand for "human proteomic data, human epigenomic data, and human metabolomic data."[163] As for the safeguarding

156 Exec. Order 14,083, 87 Fed. Reg. at 57373.

157 *See* Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, 89 Fed. Reg. 15780, 15783 (Mar. 5, 2024) (to be codified at 28 C.F.R. pt. 202).

158 *See* Exec. Order No. 14,117, 89 Fed. Reg. 15421 (Mar. 1, 2024).

159 *See* Making Emergency Supplemental Appropriations for the Fiscal Year Ending September 30, 2024, and for Other Purposes, H.R. 815, 118th Cong. div. I (2024).

160 Exec. Order No. 14,117, 89 Fed. Reg. at 15421.

161 *Id.* at 15423.

162 *Id.* at 15429.

163 *Id.* at 15428; *see* Charles Dupras & Eline M. Bunnik, *Toward a Framework for Assessing Privacy Risks in Multi-Omic Research and Databases*, 21 AM. J. BIOETHICS 46, 46 (2021) ("[R]epositories may also contain data related to other types of biological systems—often referred to as 'omics'—such as epigenomic, transcriptomic, proteomic, lipidomic, metabolomic, phenomic and microbiomic data.").

of government-related data, the executive order seeks to stop the sale of data such as the personnel data of federal employees when the sale "poses a heightened risk of being exploited by a country of concern to harm United States national security."[164]

In April 2024, Congress enacted PADFA.[165] This statute made it unlawful for a data broker "to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive information of a United States individual" to a foreign adversary country, or any entity controlled by such a country.[166] As in the TikTok Law, a company is considered controlled by a foreign adversary if persons in those specified countries directly or indirecty own at least twenty percent of the company.[167] The proposed rules implementing Executive Order 14117, by contrast, would set the ownership threshold at fifty percent.[168]

Where Executive Order 14117 gives power to the Justice Department, PADFA gives enforcement power to the Federal Trade Commission, the nation's leading federal privacy cop.[169] The law, while lacking explicit protection for "human 'omic data," adds additional categories to its definition of sensitive information. These additional groups extend to precise geolocation information; an individual's private communications; including voicemails and emails; photographs and videos of naked or undergarment-clad private areas; log-in credentials; calendar information; information about an individual under the age of 17; and "information identifying an individual's online activities over time and across websites or online services."[170]

Below, we will develop an argument regarding the shortcomings of this patchwork approach to regulating international data flows. We argue that

---

164 *See* Exec. Order No. 14,117, 89 Fed. Reg. at 15429.

165 Shortly after President Biden released Executive Order 14117, the House enacted its own measure prohibiting data brokers from transferring sensitive data of Americans to foreign adversaries. The House passed this bill by a unanimous vote. *See* Protecting Americans' Data from Foreign Adversaries Act, H.R. 7521, 118th Cong. § 2(a)-(b) (2024); Press Release, Rep. Cathy McMorris Rodgers, House Unanimously Passes McMorris Rodgers, Pallone Bill to Protect Americans' Sensitive Data (Mar. 20, 2024), https://mcmorris.house.gov/posts/house-overwhelmingly-passes-mcmorris-rodgers-pallone-bill-to-protect-americans-sensitive-data [https://perma.cc/TW2P-VE8V]. The bill was later passed by the Senate and signed by President Biden as part of an omnibus package. *See* supra note 159 and accompanying text.

166 *See* H.R. 8038 div. E § 2(a) (2024).

167 *Id.* § 2(c)(2).

168 *See* Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, 89 Fed. Reg. 15780, 15783 (Mar. 5, 2024) (to be codified at 28 C.F.R. pt. 202).

169 On the role of the FTC, see Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 147-50 (2017).

170 *See* H.R. 8038 div. E § 2(b)(7).

selecting out only certain services (TikTok and similar platforms) or business models (data brokers) is a radically underinclusive approach to national security concerns about the international flows of the personal data of U.S. citizens, and poses risks of targeting politically disfavored speech intermediaries.

* * *

A series of executive orders and implementing regulations underlie the growing executive branch power to review software and hardware for national security risks. Though some of these executive orders and regulations are ostensibly about ensuring safe supply chains for information and communications technology, their mandate extends far beyond such concerns. After all, one hardly imagines TikTok to be a key part of any supply chain. Other executive orders squarely focus on personal data, including bulk data as handled by data brokers.

Finally, Congress has spoken in this area by enacting FIRRMA and the TikTok Law. FIRRMA assigns the President strong powers to evaluate the national security risks of how foreign entities and foreign platforms collect, process, and use the personal data of Americans in the context of a foreign investment into the United States. The TikTok Law grants the President broader authority to take action regarding a variety of platforms and apps if "controlled by a foreign adversary."[171] The statute defines such an entity as being domiciled, headquartered, or principally based in a foreign country designated an adversary, or being a company in which a foreign person in such a country holds a stake of at least 20 percent.[172]

II. CONSTRAINING PRESIDENTIAL AUTHORITY OVER CROSS-BORDER DATA FLOWS

The President now claims vast regulatory power over the collection of personal information in the United States by anyone subject to the jurisdiction or direction of a foreign government. This claim rests on congressional delegation and the President's underlying constitutional authority over foreign affairs and national security. By focusing on foreign control over information and communication technology services, the executive seeks to control the cross-border flow of data. This development raises critical normative questions about the promise and risks of the national securitization of personal information.

171 H.R. 8038 div. D § 2(g).

172 *Id.*

We begin with the theoretical implications of the national securitization of personal data for privacy law, namely the emergence of a group privacy interest. We then identify legal constraints, found in existing statutes and the Constitution, on the executive branch's control over cross-border data flows. Finally, this Article develops elements of a framework for regulating this complex policy area, which we term the "National Security Constitution for Personal Data."

A. *IEEPA, CFIUS, the TikTok Law, and the Rise of Group Privacy*

The House hearing in March 2023 about TikTok manifested worries about foreign propaganda and privacy.[173] While the legislation enabling CFIUS gives the executive branch power over both, this section will now explore the contested reach of this authority under IEEPA. Moreover, due to FIRRMA, the CFIUS process has enshrined a notion of "group privacy" in American national security law. The recent IEEPA executive order blocking certain kinds of bulk sales of personal data has taken a similar path. The concept of "group privacy" as a national security value represents a notable change in American law, and one that assigns the President extensive powers using a largely untested concept.

1. Open Questions Under IEEPA, Ample Power Under CFIUS and the TikTok Law

In 1987, President Ronald Reagan stood before the Berlin Wall in West Berlin and demanded, "Mr. Gorbachev, tear down this Wall[!]"[174] Representative Howard Berman similarly sought to prevent construction of a wall, an information wall, and one that would be erected in the United States. Members of Congress promoting these amendments to IEEPA explicitly recognized the reality of foreign propaganda campaigns, but removed from the executive branch the authority to use IEEPA to block the transmission of a wide variety of information. The Berman Amendment and the Free Trade in Ideas Act demonstrate American openness during the Cold War to the free flow of information.[175]

---

173 *See* Hendrix, *supra* note 24.

174 Gerald M. Boyd, *Raze Berlin Wall, Reagan Urges Soviet*, N.Y. TIMES (June 13, 1987), https://www.nytimes.com/1987/06/13/world/raze-berlin-wall-reagan-urges-soviet.html.

175 *See* Timothy Zick, *Territoriality and the First Amendment: Free Speech at—and Beyond—Our Borders*, 85 NOTRE DAME L. REV. 1543, 1565 (2010) ("The Berman Amendment, the Free Trade in Ideas Act, and implementing regulations effectively ended the practice of seizing foreign novels, pamphlets, and magazines at the territorial border.").

The legislative history of these two amendments does not demonstrate awareness, however, of the digital transformations to come for *personal data*.[176] Absent from the congressional debate was an assessment of potential risks from foreign invasion of the privacy of Americans.[177] By the time of the second IEEPA amendment in 1994, however, the Internet was on the cusp of changes that would dramatically heighten the international transmission of personal information. In that year, Vice President Al Gore made his famous speech in which he first used the term "Information Superhighway."[178] In 1994, Amazon also registered its domain name and began to sell books online.[179] While there was little awareness of the global flow of personal data in the United States, policymakers in Europe were already concerned with privacy and the global flow of personal data. In 1989, for example, Europe's Data Protection Commissioners met in Berlin and issued a resolution calling attention to how "[i]nternational data networks are increasingly used for transfers of personal data."[180] The Berlin Resolution of August 30, 1989 demanded that the world's governments "move rapidly both individually and through international bodies towards establishing equivalent legal safeguards" for personal information.[181]

In short, any congressional contemplation of the issues regarding transborder flows of personal information was absent from the enactment of the Berman Amendment and Free Trade in Ideas Act. Because of the Berman

---

176 See CASEY, RENNACK & ELSEA, supra note 48, at 8-9 (describing the legislative concern for and associated reforms to the broad international economic power granted to the President by the Trading With the Enemy Act); *see also* S. REP. NO. 95-466, at 2 (1977) (describing the purpose of IEEPA legislation as delimiting "the President's authority to regulate international economic transactions during wars or national emergencies. The bill is a response to . . . extensive use by Presidents of emergency authority . . . unrelated to a declared state of emergency").

177 *See id.* at 5 (describing the limitations of the statute on the President's ability to regulate U.S. citizens' communications and humanitarian donations, but not speaking to foreign capture of communications or financial data).

178 *See Benton Foundation: Vice President Al Gore*, C-SPAN, at 18:04-18:12 (Mar. 29, 1994), https://www.c-span.org/video/?55624-1/information-superhighway ("Customers must be able to both receive and send information over the Information Superhighway."); *cf.* C.J. Hamelink, *Globalisation and Human Dignity: The Case of the Information Superhighway*, 43 MEDIA DEV., no. 1, 1996, at 18, 18 ("The project of the Information Superhighway envisions the incorporation of all existing communication networks into one system.").

179 *Jeff Bezos: The King of E-Commerce*, ENTREPRENEUR (May 16, 2022), https://www.entrepreneur.com/growing-a-business/jeff-bezos-biography-how-he-started-amazon-and-more/197608 [https://perma.cc/T5V7-H37L].

180 *See* Int'l Conf. of Data Prot. Comm'rs, *Berlin Resolution of 30 August 1989*, http://globalprivacyassembly.org/wp-content/uploads/2015/02/11th-ICDPPC-Berlin-1989-Berlin-Resolution.pdf [https://perma.cc/M65F-6VRE] (last visited Apr. 8, 2024).

181 *Id.* Professor Spiros Simitis, then the Data Protection Commissioner of Hessen (Germany), played a crucial role in the formulation of this resolution. *See* Paul M. Schwartz, *Spiros Simitis as Data Protection Pioneer*, 1 GW J. L. & TECH (forthcoming 2024) (manuscript at 8-9) (on file with authors).

Amendment and the Free Trade in Ideas Act, however, IEEPA cannot be used by the President to regulate, whether directly or indirectly, a long list of information media, "regardless of format or medium of transmission."[182] Yet, the plain language of IEEPA as amended leaves open questions regarding the executive branch's powers under this statute to regulate cross-border data flows. One such issue is whether the ban on indirect regulation means that the executive cannot draw on IEEPA to regulate personal data associated with an upload or download in the United States from TikTok or other foreign-owned social media.

Personal data is information, and it appears difficult conceptually, if not impossible, to disentangle personal data flows from information flows. If anything, information appears to be the larger classification, and personal data the subset of that category. Indeed, both federal courts that examined the Trump executive order and associated regulations made broad application of IEEPA's language regarding "informational materials."[183] One court flatly stated that the "informational materials" exception meant that TikTok resided in an "IEEPA-free zone."[184] After all, any government action that would either transfer ownership or ban TikTok would directly or indirectly regulate the transfer of informational materials across borders.

But even if TikTok resides in an IEEPA-free zone, that does not necessarily mean that the President lacks all power to control the flow of data under IEEPA. Consider, for example, Executive Order 14117, which also rests on IEEPA and restricts access by "countries of concern" to "Americans' bulk sensitive data and United States Government-related data."[185] A court might decide that action under Executive Order 14117 was not ultra vires by drawing a distinction between bulk databases and a speech platform. The issue would be whether a restriction on these large data sets, maintained by the data brokerage industry directly or indirectly, regulates the flow of "information or information materials." We are back to the question posed above—whether it is possible to disentangle the flow of personal data (in particular) from the flow of information (in general). A court could possibly interpret the Berman Amendment and the Free Trade in Ideas Act as focused on ensuring the free flow of expression across borders and not the transfer of large databases of personal information from the United States to a country outside its borders.

---

182 50 U.S.C. § 1702(b)(3).

183 *See* TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 112 (D.D.C. 2020) (finding the Trump Administration's TikTok ban constituted an indirect ban on informational materials under IEEPA); Marland v. Trump, 498 F. Supp. 3d 624, 641 (E.D. Pa. 2020) (holding that the TikTok ban "presents a threat to the 'robust exchange of informational materials,' and therefore comes within the scope of the informational materials exception [of IEEPA].").

184 *Marland*, 498 F. Supp. 3d at 641 (internal quotation marks omitted).

185 Exec. Order No. 14,117, 89 Fed. Reg. 15421, 15421 (Mar. 1, 2024).

As a larger matter, now that Congress has enacted the TikTok Law, IEEPA's internal limits become less important. The executive can simply make use of this new, independent statutory basis to act against a "foreign adversary controlled application." Beyond this statute, there is also the matter of executive's inherent constitutional authority. The President can argue that a "residual" foreign affairs power exists under Article II, Section I's grant of "the executive Power."[186] It is interesting to note, however, that the Justice Department did not seek to rely on any inherent executive authority to defend its TikTok ban in court in 2020.[187]

Finally, whatever the consequences of these restrictions on IEEPA prove to be, there will be ample room for executive branch action under the CFIUS process. The FIRRMA revisions to CFIUS make clear a congressional desire to protect national security, as needed, from harms due to the cross-border flow of personal data. As a policy matter then, where IEEPA may end regarding personal data, CFIUS begins—at least to the extent that the foreign action includes an investment into the United States. In turn, the Biden administration has drawn on this authority in important recent executive orders. But how does national security law now define personal data?

2. Defining Personal Data: A Confused Mixture

In furtherance of its goal of protecting national security, the laws relating to CFIUS and IEEPA have developed a broad definition of "sensitive data." Unlike the situation in the European Union, the definitions of personal information in U.S. law are a hodgepodge, a confused mixture.[188] The main takeaway, though, is that these definitions introduce a concept of group privacy into American law.

Regarding CFIUS and its approach to "sensitive data," its term of art for the personal information it seeks to protect,[189] the key language is found in the Treasury Department's regulations for FIRRMA (September 2019),

---

186 *See* Saikrishna B. Prakash & Michael D. Ramsey, *The Executive Power over Foreign Affairs*, 111 YALE L.J. 231, 234 (2001).

187 *See* Defendants' Memorandum in Opposition to Plaintiffs' Renewed Motion for a Preliminary Injunction Against Com. Dep't Prohibitions 2-5, Tiktok Inc. v. Trump, 507 F. Supp. 3d 92 (D.D.C. 2020) (No. 1:20-CV-2658-CJN), 2020 WL 6883229, at *1-2 (relying instead on "the plain text of IEEPA, binding precedent recognizing the President's broad discretion to respond to emergent national-security threats, the overall statutory scheme and purpose, and longstanding Executive Branch practice.").

188 *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1828-1835 (2011) ("Information privacy law has failed to develop a coherent and workable definition of [personally identifiable information].").

189 *See* Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1702(c)(5), 132 Stat. 2174, 2177 (2018).

issued by the Office of Investment Security (OIS),[190] and the Biden administration's Executive Order 14083 (September 2022).[191] We examine each in turn.

The OIS's FIRRMA regulations go into considerable detail regarding the parameters of "sensitive personal data" as a trigger for CFIUS review.[192] These regulations establish a complex definitional structure that begins by establishing two overarching categories. First, there is the sui generis category of genetic test results.[193] This classification provides the simplest, albeit narrowest way for information to qualify as sensitive personal data. All genetic test results fall under the regulation, and CFIUS is to be involved in evaluating the risks when foreign firms or nationals seek investment in or control of a company with access to this kind of health information.[194]

Second, the OIS regulations identify a two-pronged test for (1) certain kinds of businesses that (2) collect certain kinds of information.[195] These entities also qualify for CFIUS review. The initial part of this test covers two kinds of businesses. The first are enterprises that target their products or services to the executive branch or military, which, understandably, are classified as potentially raising national security concerns.[196] To qualify as the second kind of regulated business, a company must collect or plan to collect identifiable data on more than one million U.S. individuals during the preceding twelve months.[197] Implicit is an understanding that big databases alone can raise national security considerations.

The second required prong inquires as to whether the qualifying organization will also collect certain kinds of identifiable data. Broadly speaking, the full OIS list points to five categories of identifiable information: (1) financial data; (2) health data; (3) non-public communications; (4) geolocational data; and (5) data shared with the government to generate an identification card or obtain a security clearance.[198] The enumerated kinds of

190 *See generally* Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 84 Fed. Reg. 50174 (Sept. 24, 2019) (codified at 31 C.F.R. pt. 800).

191 *See* Exec. Order No. 14,083, 87 Fed. Reg. 57369, 57373 (Sept. 20, 2022).

192 *See* Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 84 Fed Reg. at 50174.

193 *See id.* at 50177-79 (noting that the regulation's definition "also includes all genetic information").

194 *See id.* at 50178 ("CFIUS will continue to have authority to review any transaction that could result in control by a foreign person of any U.S. business, regardless of whether the U.S. business maintains or collects sensitive personal data.").

195 *See id.* at 50189.

196 *See id.* (regulating any company that "[t]argets or tailors products or services to any U.S. executive branch agency or military department with intelligence, national security, or homeland security responsibilities").

197 *Id.*

198 *Id.*

personal data are sprawling and involve information that U.S. information privacy law may not uniformly consider to be "sensitive data." The full list of OIS categories of "sensitive data" are included in an appendix to this Article.[199] As an example, the OIS classification includes information bearing on creditworthiness as sensitive financial data, while also recognizing that many institutions regularly transmit individuals' credit information.[200]

Turning our attention to Executive Order 14083, this order defines sensitive data as "health, digital identity, or other biological data and any data that could be identifiable or de-anonymized."[201] By introducing de-anonymized information as a category of coverage, it introduces an even broader definition of "sensitive data" than that found in the OIS regulations. As the Congressional Research Service notes regarding Executive Order 14083, it "appears to promote greater scrutiny of claims that parties use only anonymized data by examining de-anonymizing capabilities."[202] In addition, the reference to "any data that could be identified or de-anonymized" seems to treat any identifiable data as "sensitive."[203]

As for IEEPA, Executive Order 14117 provides a definition of "sensitive personal data."[204] As mentioned previously, the executive order defines it as including personal identifiers, geolocational data, biometric identifiers, personal health data, personal financial data, "or any combination thereof."[205] It also extends to "human 'omic data," and, thereby, protects both genetic and molecular information.[206] Finally, Executive Order 14117 broadly safeguards "government-related data," including the personnel data of federal employees."[207]

Analysis of the TikTok Law and PADFA, the data broker law, both enacted in April 2024 similarly show a lack of consistency regarding approaches to personal data. The TikTok Law does not approach the issue of a "foreign adversary controlled application" through the prism of personal information. Instead, it permits the President authority over "covered companies" defined as certain large platforms that allow a user to create an

199 *See infra* Appendix B.

200 *See* Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 84 Fed. Reg. at 50178 (describing individual financial data that falls within the regulation's purview despite being appropriately used by companies in some instances).

201 Exec. Order No. 14,083, 87 Fed. Reg. 57369, 57373 (Sept. 20, 2022).

202 CATHLEEN D. CIMINO-ISAACS, STEVE P. MULLIGAN, & KAREN M. SUTTER, CONG. RSCH. SERV., IF12415, CFIUS EXECUTIVE ORDER ON EVOLVING NATIONAL SECURITY RISKS AND CFIUS ENFORCEMENT GUIDELINES 2 (2023).

203 *Id.*

204 *See* Exec. Order No. 14,117, 89 Fed. Reg. 15421, 15429 (Mar. 1, 2024).

205 *Id.*

206 *Id.*

207 *Id.*

account or profile and share content. In contrast, the restrictions on data brokers selling data to foreign adversaries focuses on "personally identifiable sensitive data of United States individuals."[208] As already noted above, the term "sensitive data" sweeps in a broad amount of information, including some not covered by other statutes or existing executive orders.[209]

Finally, there had been an absence of official guidance regarding the kinds of personal data that matter for foreign investment review. As a positive development, therefore, the OIS regulations, Executive Order 14034, and Executive Order 14117 heighten transparency regarding potential governmental action with respect to the scrutiny of foreign investments that implicate the gathering of personal data. At the same time, however, the OIS regulations, promulgated under CFIUS authorities, and the two executive orders promulgated under IEEPA, are not well coordinated with each other. For one thing, their definitions of personal information overlap only partially, creating uncertainty for foreign companies that might fall under executive branch scrutiny for their data-centric activities in the United States. Companies may be tripped up by differing definitions, finding themselves not engaging in a transaction involving "sensitive" data under one executive order, but then subject to scrutiny for dealing in "sensitive" data under another executive order or regulation. It is also unclear why there should be varying definitions of sensitive data for national security purposes.

3. The National Securitization of Personal Data

A group interest in privacy in the name of national security breaks new conceptual ground. First, the law has typically approached national security and the privacy of personal data as locked in opposition to each other.[210] In this traditional approach, protecting national security means engaging in surveillance and thereby limiting privacy.

Historically, the United States government has sought, with notable success, to capture the world's personal data. It has done so through collaboration with other nations, including through the "Five Eyes," an intelligence alliance with Australia, Canada, New Zealand, and the United Kingdom.[211] The United States has also massively benefited from the location

---

208 *See* 21st Century Peace Through Strength Act, H.R. 8038, 118th Cong. div. E § 2(a) (2024).

209 *See supra* notes 169-170 and accompanying text.

210 *See, e.g.*, Doe v. Holder, 665 F. Supp. 2d 426, 429 (S.D.N.Y. 2009) (adjudicating a dispute between the government and an individual from whom the government requested disclosure of another individual's personal information pursuant to a counterterrorism investigation).

211 The Trump administration even threatened the United Kingdom with exclusion from the "Five Eyes" if it did not follow U.S. policy restricting use of Huawei telecommunications equipment. HENREY FARRELL & ABRAHAM NEWMAN, UNDERGROUND EMPIRE: HOW AMERICA WEAPONIZED THE WORLD ECONOMY 99 (2023).

of critical infrastructure, including that of the Internet and the world's financial backbone, on American soil. As Henry Farrell and Abraham Newman observe, "Modern empire has turned the subterranean machineries that enable global markets and information flows . . . into tolls of coercion."[212] In their view, the United States has great power in the digital age because "the complicated wiring and plumbing arrangements of the global economy" converge on and in the United States.[213]

When it comes to national security surveillance involving the personal information of Americans, however, the law in the United States has sought to safeguard privacy—at least to some extent. Consider, for example, the ongoing debate about the renewal of Section 702 of the Foreign Intelligence Surveillance Act (FISA).[214] This FISA provision permits the U.S. government "to target non-U.S. persons, reasonably believed to be located outside the United States, in order to collect foreign intelligence information using the compelled assistance of U.S. electronic communications service providers."[215] The statutory framework also permits the communications of U.S. persons to be "incidentally" collected.[216] The Privacy and Civil Liberties Oversight Board, an independent agency within the executive branch, argues that "the United States is safer with the Section 702 program than without it."[217] Private civil liberties groups, on the other hand, argue that Section 702 infringes on the individual privacy rights of Americans.[218]

Traditionally, then, the protection of national security has meant less privacy, whether for U.S. persons or non-U.S. persons. In the case of CFIUS and IEEPA, by contrast, protecting national security means *increasing* the privacy of Americans. One essential difference between FISA Section 702 and the CFIUS and IEEPA regulations is, of course, the identity of the party doing the surveillance. In the case of FISA Section 702, the law addresses itself to how the United States government targets communications using

212 *Id.* at 3.

213 *Id.*

214 *See generally* PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2023), https://documents.pclob.gov/prod/Documents/OversightReport/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf [https://perma.cc/MZ2Y-GFML].

215 *Id.* at 2.

216 *See* 50 U.S.C. § 1805(g).

217 *See* PRIV. & C.L. OVERSIGHT BD., *supra* note 214, at 201. A majority of this agency also called for new limitations on the Section 702 program. *See id.* at 202-25 (listing nineteen recommended changes to the Section 702 program).

218 *See, e.g.*, *Warrantless Surveillance Under Section 702 of FISA*, AM. C.L. UNION, https://www.aclu.org/issues/national-security/warrantless-surveillance-under-section-702-fisa [https://perma.cc/7B64-GZDT] (last visited Apr. 8, 2024).

"selectors."[219] As for the CFIUS and IEEPA processes, the focus shifts to how foreign-controlled companies operating in the United States may gain access to virtually any kind of personal information, potentially increasing foreign government access to that data. If CFIUS decides that this data access threatens national security, it has broad powers to intervene, including ordering a forced sale of the company or the appointment of U.S. persons to leadership roles within it.[220] Thus, in the name of national security, the government may take steps to heighten privacy.

Furthermore, developments in this area go against the grain of established privacy law, which has largely resisted a collective perspective. In one of the earliest and most influential American formulations of the right to privacy, Samuel Warren and Louis Brandeis characterized this interest in 1890 as a right of each individual to protection of her "[t]houghts, emotions, and sensations."[221] Warren and Brandeis declared that privacy protected an individualized "right to be let alone."[222]

This kind of personal right is also reflected in the Supreme Court's ongoing project to heighten standing requirements under the Constitution's Article III.[223] To be able to sue for a violation of his or her privacy interests in federal court, a litigant must now demonstrate, as a threshold matter, a "concrete and *particularized*" injury.[224] Defendants have seized upon this newly heightened constitutional threshold to winnow the number of litigants in proposed class actions.[225]

---

219 *See* PRIV. & C.L. OVERSIGHT BD., *supra* note 214, at 33-34 ("[T]argeting of non-U.S. persons reasonably believed to be located outside the United States occurs with the compelled assistance of electronic communication service providers." (emphasis omitted)).

220 *See generally* 50 U.S.C. § 4565.

221 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

222 *Id.* at 193.

223 For critical discussion of these developments, see generally Paul M. Schwartz, *Privacy Standing*, 104 B.U. L. REV (forthcoming 2024) (on file with authors); Erwin Chemerinsky, *What's Standing After* TransUnion LLC v. Ramirez, 96 N.Y.U. L. REV. ONLINE 269 (2021); Danielle J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of* TransUnion v. Ramirez, 101 B.U. L. REV. ONLINE 62 (2021).

224 *See* Spokeo, Inc. v. Robins, 578 U.S. 330, 339 (2016) ("To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

225 *See* Schwartz, *supra* note 223, at 21; *see also, e.g.*, I.C. v. Zynga, Inc., 600 F. Supp. 3d 1034, 1051 (N.D. Cal. 2022) (denying standing for spam and phishing emails); Jackson v. Loews Hotels, Inc., No. ED CV 18-827-DMG, 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) ("[R]eceiving spam or mass mail does not constitute an injury."); In re Practicefirst Data Breach Litig., No. 1:21-CV-00790, 2022 WL 354544, at *5 n.8 (W.D.N.Y. Feb. 2, 2022) (determining that unsolicited spam was insufficient to constitute an injury in fact), *adopted by* No. 21-CV-790, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022).

Through standing law, the Supreme Court has demonstrated its view that privacy is to be protected on an individualized level. Indeed, one of the clearest articulations of this perspective comes in Justice Clarence Thomas's dissent in *TransUnion LLC v. Ramirez*.[226] Justice Thomas agrees with the majority that privacy is to be viewed in individualistic terms, but dissents for two reasons. First, he would find standing in that case for the entire class of plaintiffs, unlike the majority, and, second, he would do so on originalist grounds.[227] For Justice Thomas, at the time of the founding, a plaintiff could seek to enforce a privacy right by only alleging the violation.[228] And the statutory privacy rights in *TransUnion LLC*, which were expressed in the Fair Credit Reporting Act, were similarly duties "owed to a single person" and not to "the community writ large."[229] In other words, Justice Thomas viewed the originalistd understanding of statutory privacy rights as necessitating an individualist perspective on them.

To be sure, many privacy scholars have advocated for a notion of privacy as a group right. One of the authors of this Article has proposed that the law recognize privacy "as a social and not merely an individual good."[230] In a similar vein, Daniel Solove writes, "Protecting privacy can't be accomplished solely on an individualized level, as there are societal implications for many decisions that people make regarding personal data."[231] Ari Waldman states, "Individual rights will not solve collective privacy problems."[232] In her scholarship, Nancy Kim, whose work is then followed by Evan Selinger and Woodrow Hartzog, assesses data privacy through its role of protecting "collective autonomy."[233] Danielle Citron in her pioneering work regarding sexual privacy emphasizes its value not only to individuals, but to groups and society.[234] Finally, Carissa Véliz, a philosopher specializing in information

226 *See* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2217 (2021) (Thomas, J., dissenting).

227 *Id.* at 2217-18.

228 *Id.* at 2217.

229 *Id.* at 2218.

230 *See* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV 2055, 2087 (2004).

231 Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975, 987 (2023).

232 Ari E. Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. 1221, 1254 (2022) (emphasis omitted).

233 *See* NANCY KIM, CONTESTABILITY: CONSENT AND ITS LIMITS 84-88 (2019) ("State intervention is also justified to prevent the exercise of an individual's agency in order to protect another individual's greater autonomy interest or to mediate where there are conflicting autonomy interests. This approach privileges *collective* autonomy over individual autonomy where autonomy interests are equivalent." (footnote omitted)); Evan Selinger & Woodrow Hartzog, *The Incontestability of Facial Surveillance*, 66 LOY. L. REV. 33, 35 (2020) (commenting on Kim's article).

234 *See* Danielle K. Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1877 (2019).

privacy, writes, "We are responsible for each other's privacy because we are connected in ways that make us vulnerable to each other."[235]

Yet, there has not yet been much scholarly attention to the implications of government enforcement of privacy as a group right in the context of data collection by foreign-owned private sector companies.[236] In particular, there are new risks when privacy is protected in the name of national security. The question is when and how foreign-owned companies' access to the personal data of Americans threatens the security of the economy, institutions, and citizens of the United States. As noted, one problem is that the definitions of the types of personal information that matter are now sprawling, inconsistent, and nearly limitless. Second, the relevant statutory approaches to national security and peacetime national emergencies, which center on foreign ownership, are an underinclusive approach to this task.

Even without foreign ownership, major platforms and social media are subject to data collection risks. Consider the matter of data brokers.[237] As discussed above, the recently enacted PADFA gives the Federal Trade Commission the power to stop data brokers from transferring the sensitive personal data of Americans to foreign adversaries.[238] In addition, Executive Order 14117 gives the Executive power to block data brokers from selling or transferring "bulk sensitive data" to foreign adversaries.[239] The Department of Justice has announced in its Advanced Notice of Proposed Rulemaking that it will proceed by identifying "certain bulk-volume thresholds."[240] The proposal sets special rules for government-related data. Different kinds of sensitive personal data will be classified along a sliding scale with human genomic data protected potentially once a data set involves more than 100

235 *See* CARISSA VÉLIZ, THE ETHICS OF PRIVACY AND SURVEILLANCE 170 (2024).

236 *See, e.g.*, David Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 229 (2016) (discussing how policy may shift privacy burden or benefits among groups that suffer privacy harms as well as groups that cause harm to a certain privacy interest); Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 521 (2017) (discussing the need in the context of cybersecurity to "preserve privacy as a public value").

237 Already in 2012, the Federal Trade Commission called for Congress to enact legislation mandating that data brokers give consumers access to their data. *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, at viii (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/4RYD-WD9N]; *cf.* Alicia P. Cackley, *Personal Information, Private Companies*, U.S. GOV'T ACCOUNTABILITY OFF. (May 1, 2018), https://www.gao.gov/blog/2018/05/01/personal-information-private-companies [https://perma.cc/EYH3-QTHT] (recommending that Congress strengthen the current framework with regards to personal data collection).

238 *See supra* notes 166–168 and accompanying text.

239 *See* Exec. Order 14,117, 89 Fed. Reg. 15421, 15421 (Mar. 1, 2024).

240 *See* Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, 89 Fed. Reg. 15780, 15783 (Mar. 5, 2024) (to be codified at 28 C.F.R. pt. 202).

persons and personal financial data potentially somewhere between more than 1,000 U.S. persons or more than one million U.S. persons.[241] Setting regulatory triggers very low will interfere with the information sharing needed for medical research or disease control, or financial information sharing needed for routine transactions or customer management.

Yet, even after PADFA and Executive Order 14117, it may remain possible to obtain bulk personal data from U.S.-owned companies—even without acquiring a U.S. enterprise. In a detailed analysis of the executive order, for example, Peter Swire and Samm Sacks express deep skepticism about whether "the new order will actually meet its stated national security goal of blocking adversary access to the data of Americans."[242] Among their concerns, Swire and Sacks point to a number of "difficult-to-stop" loopholes and the ability of foreign adversaries to engage in "side channel attacks" involving non-regulated data.[243] As an illustration, "Even without any direct access to medical data, for instance, any of the myriad apps that collect location data might be used to pinpoint if a woman has visited a reproductive clinic."[244]

From *Hans Brinker, or the Silver Skates* (1865), Americans know the fictional story of the Little Dutch Boy who saved a city by putting his finger in a dike.[245] As it turns out, that is an unlikely strategy to stop flooding, because dikes generally fail through the collapse of entire sections and not leakage through small holes.[246] Similarly, international data flows are highly porous in the digital age. PADFA and Executive Order 14117 represent an attempt to plug the source of some leaks.[247]

The day after issuing Executive Order 14117, the Biden administration continued this patchwork approach by turning to data flows through foreign automobiles in the United States. On February 29, 2024, it announced a Department of Justice rulemaking to investigate connected cars from "countries of concern." It stated:

---

241 *Id.* at 15786.

242 *See* Peter Swire & Samm Sacks, *Limiting Data Broker Sales in the Name of U.S. National Security: Questions on Substance and Messaging*, LAWFARE (Feb. 28, 2024, 8:38 PM), https://www.lawfaremedia.org/article/limiting-data-broker-sales-in-the-name-of-u.s.-national-security-questions-on-substance-and-messaging [https://perma.cc/22TW-TGV6].

243 *Id.*

244 *Id.*

245 *See generally* MARY MAPES DODGE, HANS BRINKER, OR THE SILVER SKATES: A STORY OF LIFE IN HOLLAND (Charles Scribner's Sons, 1909) (1865). For background on this story, see generally Bart Schultz, *The Story of the Dutch Boy Who Prevented a Flooding Disaster: Origins and Variations on a Theme*, 11 WATER HIST. 207 (2019).

246 Due to climate change, the situation of catastrophic dam failure is particularly acute in California, where embankment dams have layers that "can melt away at an astonishing speed." *See* Christopher Cox, *The Trillion-Gallon Question*, N.Y. TIMES MAG. (July 21, 2023), https://www.nytimes.com/2023/06/22/magazine/california-dams.html [https://perma.cc/55TP-KG2N].

247 *See generally* Exec. Order No. 14,117, 89 Fed. Reg. 15421 (Mar. 1, 2024).

> Connected vehicles collect large amounts of sensitive data on their drivers and passengers; regularly use their cameras and sensors to record detailed information on U.S. infrastructure; interact directly with critical infrastructure; and can be piloted or disabled remotely. Connected autos that rely on technology and data systems from countries of concern, including the People's Republic of China, could be exploited in ways that threaten national security.[248]

As with singling out bulk data, a focus on connected automobiles is underinclusive. By this logic, we should now expect targeted rulemaking directed at connected refrigerators, washing machines, dishwashers, fitness watches, toasters, televisions, and toothbrushes. A fuller policy response to these threats will require enactment of a federal information privacy law for the private sector.[249]

There is also the risk of foreign propaganda. Here, too, a focus on foreign ownership—or even direction—is an underinclusive tactic. For example, consider some important non-foreign-owned enterprises. Putin's Russia is known to have used American social media during the 2016 election to advance its interests.[250] X (formerly Twitter) played a similar role in the 2016 election and has recently engaged in a series of staff reductions that may reduce its ability to spot foreign disinformation.[251]

Finally, core First Amendment concerns may limit the U.S. government's ability to take action in the name of group privacy. In *Sorrell v. IMS Health, Inc.*, a case to which we will return in the next Section, the Supreme Court said, "Privacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the

---

248 Press Release, White House, Fact Sheet: Biden-Harris Administration Takes Action to Address Risks of Autos from China and Other Countries of Concern (Feb. 29, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/29/fact-sheet-biden-harris-administration-takes-action-to-address-risks-of-autos-from-china-and-other-countries-of-concern [https://perma.cc/4Y89-YWDC].

249 *See, e.g.*, Robert D. Williams, *To Enhance Data Security, Federal Privacy Legislation is Just a Start*, BROOKINGS INST. (Dec. 1, 2020), https://www.brookings.edu/articles/to-enhance-data-security-federal-privacy-legislation-is-just-a-start [https://perma.cc/W6EP-QDXJ].

250 *See* S. REP. NO. 116-290, vol. 1, at 69 (2020) ("The Internet Research Agency—an entity with ties to Russian President Vladimir Putin—used social media to sow disinformation and discord among the American electorate.").

251 *See* Patrick Tucker, *Musk Has Reduced Twitter's Ability to Spot Foreign Disinformation, a Former Data Scientist Says*, DEFENSE ONE (Dec. 21, 2022), https://www.defenseone.com/technology/2022/12/musk-has-reduced-twitters-ability-spot-foreign-disinformation-former-data-scientist-says/381185 [https://perma.cc/6PGA-82J4] ("It's not clear how Twitter can filter out foreign disinformation now that CEO Elon Musk has gutted the teams meant to prevent a repeat of Russia's effort to sway the 2016 presidential election, says one former Twitter senior data scientist.").

government prefers."[252] In that case, the Court invalidated a Vermont statute that limited the ability of pharmacists to share personal information with pharmaceutical companies.[253] This law's fatal flaw for First Amendment purposes was its singling out of *one party* for restrictions on information sharing, that is, speech.[254] Like the Vermont statute, the rules targeting cross-border data flows also block information sharing with particular actors, potentially triggering heightened scrutiny under the First Amendment. We now further explore the issue of constitutional and other legal constraints on the executive branch.

B. *Statutory and Constitutional Constraints*

This Section considers current statutory and constitutional constraints in place on presidential power over cross-border data flows. An agency action, even one taken on the basis of alleged congressional authorization and performed in the name of national security, can be challenged either because it adopts a "mistaken view of the law or because it fails to provide constitutionally required due process."[255] We begin with the constraints set out in IEEPA, which is the chief statute underpinning the executive orders and regulations at issue. We then turn to the constraints found in the First Amendment's free speech clause and in the Fifth Amendment's due process clause.[256]

1. Statutory Constraints

Parties harmed by executive agency actions can seek judicial review of those measures on the ground that they exceed the agency's statutory authorization or otherwise conflict with a statute.[257] An ultra vires claim is

---

252 *See* Sorrell v. IMS Health, Inc., 564 U.S. 552, 580 (2011).

253 *See id.*

254 *See id.* at 578-80.

255 *See* Huawei Techs. USA, Inc. v. Fed. Commc'ns Comm'n, 2 F.4th 421, 460 (5th Cir. 2021) (rejecting Huawei's challenge to an agency order barring it from government subsidies on grounds that it posed a security risk).

256 The Montana TikTok ban raises yet another constitutional issue—whether a state's ban on a foreign app intrudes on either the foreign affairs or commerce powers of the federal government. *See* Nat'l Foreign Trade Council v. Natsios, 181 F.3d 38, 77 (1st Cir. 1999) (holding that Massachusetts could not block all commerce with a foreign nation under various constitutional and statutory provisions), *aff'd*, Nat'l Foreign Trade Council v. Crosby, 530 U.S. 363 (2000).

257 *See* Fed. Express Corp. v. U.S. Dep't of Com., 39 F.4th 756, 763 (D.C. Cir. 2022) (entertaining challenge to an agency action issued under the Export Controls Act on the ground that the agency's interpretation violated the statute, but ultimately upholding the action as consistent with the statute); *cf.* Chamber of Com. of U.S. v. Reich, 74 F.3d 1322, 1339 (D.C. Cir. 1996) (upholding a challenge to an executive order because it conflicted with a statute). It is "clear beyond cavil . . . that executive orders that conflict with the purposes of a federal statute are *ultra*

> available where (i) there is no express statutory preclusion of all judicial review; (ii) "there is no alternative procedure for review of the statutory claim; and (iii) the agency plainly acts in excess of its delegated powers and contrary to a specific prohibition in the statute that is clear and mandatory.[258]

The Administrative Procedure Act (APA) also empowers a court to consider whether an agency action is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" or "in excess of statutory . . . authority."[259]

Two federal courts have now found that the Trump administration's actions to ban TikTok, taken pursuant to IEEPA, were ultra vires. These decisions rested on the Berman Amendment and Free Trade in Ideas Act. First, in *Marland v. Trump*, a case from the Eastern District of Pennsylvania, the court found that the executive order shutting down TikTok was ultra vires because TikTok existed to facilitate communication; the Secretary of Commerce's prohibitions on it in the executive order aimed to stop these communications; and the Berman Amendment and Free Trade in Ideas Act sought to prohibit precisely such actions.[260] As the court observed, if TikTok were banned, "Plaintiffs [would] no longer be able to export their comedy, music, and fashion videos, and [would] no longer be able to view videos from TikTok's substantial global user base which, as of this writing, consists of at least 600 million users."[261]

Second, in *TikTok Inc. v. Trump*, the District Court for the District of Columbia held that the availability of CFIUS was key to understanding the reach of IEEPA.[262] In particular, the Trump administration's action was arbitrary and capricious under the APA because the contested executive order did not reflect the presence of less detrimental alternatives to shutting down TikTok.[263] The court pointed to the potential of resolving the national security concerns aired in the executive order through other "obvious alternative[]" means, including "a parallel divestment process."[264] That parallel action could take place through CFIUS. The *TikTok* court observed, "The Secretary [of Commerce] is not in charge of the CFIUS process . . . but

---

vires."); Am. Fed'n of Gov't Emps. v. Trump, 318 F. Supp. 3d 370, 417 (D.D.C. 2018), *rev'd on other grounds and vacated*, 929 F.3d 748 (D.C. Cir. 2019).

258 *Fed. Express Corp.*, 39 F.4th at 763 (quoting Nyunt v. Chairman, Broad. Bd. of Governors, 589 F.3d 445, 449 (D.C. Cir. 2009)).

259 *See* 5 U.S.C. §§ 706(1)(A), (C).

260 *See* 498 F. Supp. 3d 624, 640-41 (E.D. Pa. 2020).

261 *Id.* at 637.

262 *See* 507 F. Supp. 92, 111-12 (D.D.C. 2020) (identifying the importance of CFIUS under the IEEPA).

263 *Id.* at 112.

264 *Id.* at 111.

he is not free to ignore an obvious alternative available to him simply because it has some relationship to proceedings before another executive agency."[265]

This case law points to a fatal flaw in the bulk of the executive orders and regulations in this area, which rest on IEEPA and not CFIUS. These orders and regulations purport to grant the power to ban information services or to require mitigation measures, including various controls, on such services. Moreover, the Supply Chain Rule permits the Secretary of Commerce to ban an information and communications technology and services transaction if it involves a person who is "subject to the jurisdiction or direction of a foreign adversary" and the Secretary determines that it poses a "undue or unacceptable risk."[266] But this rule as well as the bulk of the executive orders and accompanying regulations do not exclude any such action by the executive if it would directly or indirectly regulate informational materials.[267]

Executive orders and regulations cannot grant the President or an agency a power that the underlying statute declined to bestow.[268] Because IEEPA excludes such powers over informational materials, any effort to exercise an authority granted by an executive order or regulation that would directly or indirectly regulate informational materials is vulnerable for attack as being ultra vires. In the context of a regulatory action against a massive speech platform such as TikTok, such a step may well be ultra vires. But the matter is more complex when the target of the regulatory activity does not directly involve speech.

For example, consider Executive Order 14117 regarding bulk sales of sensitive data and PADFA, a statutory approach, to the same issue of data brokers. As noted previously, a court might decide that action under Executive Order 14117, which rests on IEEPA, was not ultra vires by drawing a distinction between bulk databases and a speech platform.[269] In this fashion, a court might disentangle the flow of personal data (in particular) from the flow of information (in general), though a court could equally conclude that the two are not logically distinguishable.

---

265 *Id.*

266 Securing the Information and Communications Technology and Services Supply Chain, 15 C.F.R. §§ 7.100(c)-(d) (2024).

267 The Supply Chain Rule does repeatedly mention "information and documentary materials," but only to assure parties that submit confidential information in the context of any review that the information would be released only in very narrow circumstances. *See, e.g.*, *id.* § 7.102(a).

268 *See* GRABER, *supra* note 124, at 1 ("To have legal effect, an executive order must have as its source of authority either the President's powers in Article II of the Constitution or an express or implied delegation of power from Congress to the President . . . . [N]o statute grants the President the general authority to issue executive orders.").

269 *See supra* note 185 and accompanying text.

The issue of a challenge on the basis of ultra vires action will not be present regarding PADFA. That law squarely takes aim at the sale by data brokers of sensitive personal information to a foreign adversary or a company controlled by such a country. In that context, however, First Amendment lawsuit will still be possible. Indeed, in *Sorrell v. IMS Health Inc.*, the Supreme Court treated the sharing of prescription records as speech protected by the First Amendment.[270] In *Sorrell*, the Court objected to the singling out of a group of speakers—namely, pharmacies and pharmaceutical companies.[271] Similarly, a court reviewing PADFA might find that it targets a single group, data brokers, and hence, is a content-based regulation subject to strict scrutiny. And that kind of analysis usually proves fatal for any regulation subject to judicial review.

Any litigation victory by a regulated entity based on this approach is likely, however, to be a pyrrhic one if the transaction involves not data brokers, but a foreign investment in the United States due to FIRRMA's revision of the CFIUS authorities. FIRRMA makes it clear that Congress has authorized the President to regulate cross-border flows of "sensitive data."[272] And the Biden administration's Executive Order 14083, which concerns "sensitive data," rests on CFIUS rather than IEEPA.[273] The statutory grant of powers to regulate data flows through the CFIUS legislation is vast.

Indeed, while the statutory timeline for CFIUS review envisions a 105-day timeline from start to finish for the CFIUS process, the reality is different than the law on the books.[274] As one law firm with a practice in the area explains, "While the 30-day and 45-day periods for initial reviews and investigations are helpful guideposts when thinking about a transaction timeline, they do not offer parties any certainty."[275] CFIUS has ways of informally resetting the regulatory clock, namely by requesting that parties withdraw and refile their notice, which begins the time period anew.[276] As an

---

270 *See* 564 U.S. 552, 557 (2011).

271 *See id.* at 562-63.

272 *See* Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1702(c)(5), 132 Stat. 2174, 2177 (2018) (authorizing the regulation of flows of sensitive data of U.S. citizens).

273 *See* Exec. Order No. 14,083, 87 Fed. Reg. 57369, 57373 (Sept. 20, 2022).

274 *See CFIUS Overview*, COOLEY, https://www.cooley.com/services/practice/cfius/cfius-overview [https://perma.cc/EDU8-B7QV] (last visited Apr. 10, 2024) ("A [CIFUS] Notice is a more comprehensive and detailed submission with lengthier 'review' and 'investigation' periods that collectively can last between 45 and 105 days.").

275 *M&A Guide to CFIUS: Deciding Whether to Submit Voluntarily to CFIUS Review*, COOLEY (Feb. 27, 2018), https://www.cooley.com/news/insight/2018/2018-02-27-ma-guide-to-cfius [https://perma.cc/6NJT-59XP]. This explanation is a considerable understatement.

276 *Id.*

illustration, the CFIUS investigation of TikTok is now entering its fifth year.[277]

While FIRRMA's grant of authority over sensitive information is broad, a First Amendment challenge will still be available to action taken pursuant to it. A contrast can be drawn between FIRRMA and the Berman Amendment and Free Trade in Ideas Act. The latter seek "[t]o restrict the authorities of the President with respect to regulating the exchange of information with . . . foreign countries."[278] The resulting information materials exception that these amendments add to IEEPA is, at some level, an effort to build First Amendment's safeguards into this statute.

The Berman Amendment and Free Trade in Ideas Act insert a First Amendment safety valve into the larger statutory framework of IEEPA. But the TikTok Law as well as the executive orders and regulations described above in Part I, even those based on IEEPA authorities, do not add any such First Amendment safeguards to their authorizations—they do not exclude from their reach the power to regulate directly or indirectly informational materials. Federal courts will ultimately be the judge of the reach of the First Amendment in this area, and we turn now to this issue.

2. First Amendment Constraints and the Executive's Power over Foreign Affairs

Through IEEPA, Congress has readily granted the executive power over the outbound flows of the personal data of Americans (with a notable limit in the Berman Amendment and the Free Trade in Ideas Act). The TikTok Law is a further manifestation of the trend of a congressional grant to the executive authority over cross-border data flows. In his famous *Youngstown* concurrence, Justice Jackson spoke of a situation where "the President acts pursuant to an express or implied authorization of Congress," and noted that here "his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate."[279] A ban of TikTok by the President would be pursuant to an express authorization of Congress.

Nonetheless, even in that situation, limits exist on the power of the President. In his *Youngstown* concurrence, Justice Jackson argued that, even when acting pursuant to an act of Congress, presidential action becomes unconstitutional when "the Federal Government as an undivided whole lacks

277 *See generally Issues Over TikTok Still Unresolved, US Treasury Secretary Yellen Says*, REUTERS (Nov. 20, 2023, 8:40 AM), https://www.reuters.com/technology/issues-over-tiktok-still-unresolved-us-treasury-secretary-yellen-says-2023-11-20.

278 Free Trade in Ideas Act of 1992, H.R. 5406, 102d Cong. (1992); *see also supra* Section I.B; Berman Amendment, Pub. L. No. 100-418, § 2502, 102 Stat. 1371 (1988).

279 Youngstown Sheet & Tube Co v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring).

power."[280] Congress cannot delegate to the President a power that it lacks.[281] Congress cannot grant the executive unconstitutional powers. Indeed, the executive's constitutional powers, explicit or inherent, can also conflict with other constitutionally protected interests. These limitations are especially important when it comes to the regulation of personal information by the President.

One federal court has already examined this issue. This decision occurred in the context of the Trump administration's ban of WeChat, a messaging, social media, and mobile payment application. Rather than relying on IEEPA's "information material exclusion," this court held that Executive Order 13943 likely violated the First Amendment rights of WeChat users, who were predominately Chinese American and Chinese-speaking users.[282] Users of WeChat had argued that it provides important content, such as the news in Chinese, and resonates culturally with its users "because it integrates Chinese traditions into electronic transactions, such as sending gifts of money in 'red envelopes.'"[283] The users had also made declarations showing that WeChat was their primary source of communication and commerce in part because China blocked many western social media platforms, such as Facebook, WhatsApp, and Twitter, which made WeChat the only way for its users in the United States to reach their networks in China.[284] The app was "effectively the only means of communication for many in the community," and these users had raised serious questions showing that the executive order would "effectively eliminate [their] key platform for communication, slow or eliminate discourse, and [was] the equivalent of censorship of speech or a prior restraint on it."[285]

It is ironic, to be sure, that Chinese government censorship in China helped heighten the First Amendment protections for WeChat users in the United States. But the First Amendment protects the ability of WeChat users of the Chinese community in the United States to communicate with those inside and *outside* of the United States.[286] Indeed, it would be equally ironic if the First Amendment did not protect Chinese Americans from speech app bans in the United States.[287]

---

280 *Id.* at 636-37.

281 *Id.*

282 *See* U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912, 917-18 (N.D. Cal. 2020).

283 *Id.* at 918.

284 *Id.*

285 *Id.* at 926-27.

286 *See* Zick, *supra note* 175, at 1559 ("[T]he Supreme Court has grudgingly assumed that 'First Amendment protections reach beyond our national boundaries.'" (citing Haig v. Agee, 453 U.S. 280, 308 (1981)).

287 Another successful First Amendment claim in the national security area concerned restrictions levied by a Trump administration executive order that set up transactions against

A federal court also found similar First Amendment protection for a social media platform faced with a state ban—as opposed to action resting on executive branch authority. In *Alario v. Knudsen*, the District Court for the District of Montana, applying intermediate scrutiny to a Montana statewide TikTok ban, declared that the contested Montana law "completely shuts off TikTok to Montana users."[288] The court held that TikTok involves "traditional First Amendment speech."[289] TikTok was a "means of expression" for its users, and at the same time reflected TikTok's own speech as it "selects, curates, and arranges content."[290]

Recent Supreme Court precedent has also identified strong First Amendment protections when Congress acted to protect privacy by limiting the flow of information. As noted in the preceding Section, the *Sorrell* Court found that a Vermont statute was unconstitutional because it singled out one party, pharmacists, for restrictions on their sharing of personal information with pharmaceutical companies.[291] Their distribution of this information was speech safeguarded by the First Amendment.[292]

In the case of the Trump administration's attempted restrictions on TikTok, the aim was to protect the group privacy of users by limiting their own information sharing.[293] Presumably, some or many of these users, like the pharmacists who litigated in *Sorrell*, would be against this restriction on their communication. This issue is now again a live one with the enactment of the TikTok Law. While it is unclear how a court would decide this kind of litigation, there are significant constitutional claims for both parties. The government will argue in favor of its group privacy protections, which sound in the President's power to protect national security, and TikTok users will seek to protect their First Amendment interests.

Three other Supreme Court cases, two from the Cold War era and one from the current War on Terror, have tested the limits of regulations on cross-border information flows. The lessons from these cases are, first, that the First

individuals, including U.S. law professors, who were associated with the International Criminal Court. A district court found that the executive order was not narrowly tailored and, hence, unconstitutional under strict scrutiny review. *See* Open Soc'y Just. Initiative v. Trump, 510 F. Supp. 3d 198, 213 (S.D.N.Y. 2021).

288 No. CV 23-56-M-DWM, 2023 WL 8270811, at *8 (D. Mont. Nov. 30, 2023).

289 *Id.* at *6.

290 *Id.*

291 *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 580 (2011).

292 *Id.* at 557 ("Speech in aid of pharmaceutical marketing, however, is a form of expression protected by the Free Speech Clause of the First Amendment. As a consequence, Vermont's statute must be subjected to heightened judicial scrutiny. The law cannot satisfy that standard.").

293 *See* Exec. Order No. 13,942, 85 Fed. Reg. 48637, 48637-38 (Aug. 11, 2020) (attempting to prohibit, in U.S. jurisdictions, any transactions with ByteDance Ltd., Beijing, China, or its subsidiaries, as specified by the Secretary of Commerce under section 1(c) of the order, in accordance with applicable law).

Amendment includes a right to hear foreign views, and, second, that a registration and labeling of foreign "political propaganda" may be permissible.[294] In *Lamont v. Postmaster General* (1965), American citizens challenged a federal law that imposed restrictions on their ability to receive material from China.[295] A 1962 statute had required the U.S. Postal Service to detain all "communist political propaganda" entering the shores, and then ask the addressee whether they would indeed like to receive the material.[296] The Supreme Court unanimously struck down this law with Justice William Douglas explaining, "The Act sets administrative officials astride the flow of mail to inspect it, appraise it, write the addressee about it, and await a response before dispatching the mail."[297] As a commentator on the case observed, "This right to receive information does not disappear when the information being received comes from abroad, nor does it become less vital."[298]

Two decades later, the Court would find permissible a different kind of statute regulating foreign information. In the 1987 case of *Meese v. Keene*, the Supreme Court upheld the constitutionality of a law requiring registration and labeling of foreign "political propaganda."[299] But it did so only after concluding that the registration and labeling statute "places no burden on protected expression" nor "any obstacle" to distribution.[300] The Court observed that "Congress did not prohibit, edit, or restrain the distribution of advocacy materials in an ostensible effort to protect the public from conversion, confusion, or deceit."[301]

In 2010, the Supreme Court considered a First Amendment challenge in the context of the War on Terror. In *Holder v. Humanitarian Law Project*, plaintiffs challenged the sanction authorities granted by the Antiterrorism and Effective Death Penalty Act, which permits the State Department to designate an entity as a Foreign Terrorist Organization (FTO).[302] The law prohibits the provision of "material support or resources" to any entity

294 *See* Meese v. Keene, 481 U.S. 465, 481 (1987) ("By compelling some disclosure of information and permitting more, the [Foreign Agents Registration] Act's approach recognizes that the best remedy for misleading or inaccurate speech contained within materials subject to the Act is fair, truthful, and accurate speech.").

295 381 U.S. 301, 304 (1965).

296 *Id.* at 302.

297 *Id.* at 306.

298 Nadia L. Luhr, *Iran, Social Media, and U.S. Trade Sanctions: The First Amendment Implications of U.S. Foreign Policy*, 8 FIRST AMEND. L. REV. 500, 518 (2010).

299 *See* 481 U.S. at 467-69 (holding that the Foreign Agents Registration Act's use of the term "political propaganda" is constitutional in that the Act's use of the term is neutral).

300 *Id.* at 480.

301 *Id.*

302 *See* 561 U.S. 1, 7-8 (2010).

designated an FTO.[303] Plaintiffs argued that the law infringed on their First Amendment rights.[304] Applying strict scrutiny, the Supreme Court upheld the law as applied to the plaintiffs. It vindicated the congressional refusal in the statute to segregate support of legitimate activities of an FTO from their terrorist acts.[305] The Court majority insisted that it was not abdicating its judicial role, but, rather, was simply being cognizant of how "national security and foreign policy concerns arise in connections with efforts to confront evolving threats in an area where information can be difficult to obtain and the impact of certain conduct difficult to assess."[306]

It is unclear whether the Supreme Court would give similar deference in the First Amendment context to an executive branch ban on TikTok or similar foreign platforms. On one hand, *Holder* was a case about interactions with designated "foreign terrorist organizations."[307] The majority observed that "[t]he PKK and LTTE have committed terrorist acts against American citizens abroad."[308] Whatever its national security risks, TikTok, the home of dance challenges and beauty trends, is hard to equate with groups that carry out terrorist attacks. Hence, the Court's frame for assessing the case is likely to be different from when it considers measures relating to the ongoing efforts of the post 9/11 War on Terror.

Finally, there are novel First Amendment claims raised by the CFIUS power to appoint proxy boards consisting of U.S. persons to foreign-owned corporation. In fact, TikTok's Project Texas is said to be in talks with CFIUS to have the company "cede authority over TikTok's U.S. operations to a three-person board whose members CFIUS would essentially select."[309] TikTok appears to have agreed that its new sub-entity, TikTok USDS, will be "run by the CFIUS-approved board that would report solely to the federal government, not ByteDance."[310] Government approval rights over the board of directors of a company that manufactures electronics for the U.S. military do not raise the same speech concerns as such rights over a company like TikTok.[311] A communications company that refused such a measure might

303 *Id.* at 8.

304 *Id.*

305 *Id.* at 33-39.

306 *Id.* at 34.

307 *See id.* at 8.

308 *Id.* at 34.

309 Drew Harwell, *TikTok and U.S. Rekindle Negotiations, Boosting App's Hopes for Survival*, WASH. POST. (Sept. 15, 2023, 7:00 AM), https://www.washingtonpost.com/technology/2023/09/15/tiktok-ban-us-negotiations [https://perma.cc/4YRX-MVYQ].

310 *Id.*

311 For example, an Italian company's acquisition of a U.S. electronics supplier to the U.S. military involved certain conditions with respect to the U.S. subsidiary's board of directors. *See* Paolo Biondi & Robin Pomeroy, *Finmeccanica to Buy DRS for $5.2 Billion*, REUTERS (May 13, 2008,

argue, in accord with *Lamont*, that its speech and the speech of its users were violated by having board members approved by the Executive Branch set astride their flow of communications.

3. Due Process Constraints

As the preceding section on First Amendment restraints on national security powers demonstrates, the executive does not have plenary, all-but-unreviewable power over national security, even when supported by legislation. Indeed, the First Amendment is likely to be a powerful source of future claims regarding executive branch actions to restrict the collection and use of personal data by foreign-owned social media apps in the United States. A second potential constraint on the exercise of executive authority over national security arises out of the Fifth Amendment's Due Process Clause. Due process is required before adverse action can be taken against a person, though the extent of these protections is a highly contested question when the decision implicates national security.

Notably, due process claims against executive national security actions did not gain traction when the federal courts considered the bans on Twitter or WeChat.[312] Moreover, in IEEPA and CFIUS cases, courts typically find that some kind of due process rights exist in the national security context, but that the government acted constitutionally in the kind of process provided. For example, a number of cases have considered the extent of permissible government secrecy. In 2014, Twitter sought to publish a transparency report indicating the aggregate number of foreign intelligence surveillance orders that it had received in the previous six months, and to do so only through broad disclosure categories.[313] The Ninth Circuit Court rejected a due process challenge based on the government's refusal to share material with Twitter's lead outside counsel.[314] It found that (1) the material was classified; (2) a lower court had reviewed the material in camera without finding any due process concern; and (3) "[t]he unclassified declarations provided Twitter

7:26 AM), https://www.reuters.com/article/idUSL12267658 [https://perma.cc/P6KV-ABJD] ("DRS will operate as a wholly-owned subsidiary, maintaining its current management and headquarters with a board comprised predominantly of U.S. citizens holding security clearances that will allow it to comply with security requirements, the statement said.").

312 *See, e.g.*, Twitter, Inc. v. Garland, 61 F.4th 686, 690 (9th Cir. 2023) ("We [] hold that the statutory scheme governing the permissible disclosure of aggregate data about the receipt of national security legal process allows for sufficient procedural protections, which Twitter received here.").

313 *See id.* at 693 (noting that, in its transparency report, Twitter sought to disclose detailed information about the NSLs and FISA orders it received from July to December 2013, including their number in specified ranges, comparisons with authorized ranges and other providers, and a descriptive statement on its national security surveillance exposure).

314 *See id.* at 711 (holding that Twitter's interest in the classified information does not rise to the level of constitutional imperative).

with sufficient information by which to advance Twitter's interests before this Court."[315]

As for case law regarding the limits of executive power to review inbound investments for national security risks, we are obliged to parse the lessons of *Ralls Corporation v. Committee on Foreign Investment in the U.S.*[316] Most corporations that have been targeted by CFIUS abide by that committee's orders. The only company to directly challenge a CFIUS order has been the Ralls Corporation, a Delaware corporation owned by two Chinese citizens.[317] In that case, the government argued that the CFIUS divestiture order was unreviewable because the statute itself includes a finality provision that states, "The actions of the President . . . and the findings of the President . . . shall not be subject to judicial review."[318] The district court held that this finality provision foreclosed the statutory ultra vires challenge.[319]

More controversially, the court agreed that the finality provision also foreclosed an equal protection challenge because adjudicating that challenge would effectively require the court to adjudicate the wisdom of the action, which it refused to do.[320] The district court concluded, however, that the finality provision did not bar the due process claim, which "raises a pure legal question that can be answered without second-guessing the President's determinations."[321] On appeal, the government argued that, according to the political question doctrine, the court was barred from considering the corporation's claim that due process required it to gain access to evidence that

315 *Id.* Before this case was decided, one author observed, "Courts have largely developed due process requirements [for entities that fund terrorism], but they have not yet determined what process is due when the president employs IEEPA to blacklist entities posing information-based national security threats." *See* Jonathan W. Ellison, *Trust the Process? Rethinking Procedural Due Process and the President's Emergency Powers over the Digital Economy*, 71 DUKE L.J. 499, 515 (2021).

316 *See* 926 F. Supp. 2d 71 (D.D.C. 2013) (examining the legality of the Defense Production Act of 1950, which prohibited Ralls Corporation, owned by Chinese nationals, from acquiring windfarm projects near a U.S. Naval installation in Oregon for national security reasons).

317 See, for example, the case of Beijing Kunlun Tech (BKT) and its dating app Grindr, where CFIUS demanded BKT sell its 60% stake in the company. Zack Whittaker, *Grindr Sold by Chinese Owner After US Raised National Security Concerns*, TECH CRUNCH (Mar. 6, 2020, 1:06 PM), https://techcrunch.com/2020/03/06/grindr-sold-china-national-security [https://perma.cc/5W7C-FDHW]. Similarly, a 2018 executive order blocking the takeover of Qualcomm Incorporated by Broadcom Limited required the parties to "provide a certification of termination of the proposed takeover to CFIUS." *See* Regarding the Proposed Takeover of Qualcomm Incorporated by Broadcom Limited, 83 Fed. Reg. 11632, 11632 (Mar. 15, 2018).

318 *See Ralls Corp.*, 926 F. Supp. 2d at 86; *see also* Defense Production Act of 1950, 50 U.S.C. app. § 2170(e).

319 *See Ralls Corp.*, 926 F. Supp. 2d at 91.

320 *Id.* at 94.

321 *Id.* at 95.

led to the divestiture order and an opportunity to rebut that evidence.[322] The D.C. Circuit Court of Appeals, citing *Marbury v. Madison*, held that such procedural challenges were well within judicial purview.[323] The D.C. Circuit also remanded Ralls' other challenges to the CFIUS order, including the APA, ultra vires, and equal protection challenges, to the district court for merits review.[324]

C. *Responding to the National Securitization of Personal Data*

In thinking through paths to limiting executive power over national security, we first turn to the respective scholarship of Harold Koh and Jack Goldsmith. This Article then concludes with suggestions regarding initial steps towards a National Security Constitution for Personal Data as well as topics for future research.

1. The National Security Constitution for Personal Data

The nature of limits, constitutional and otherwise, on the President's national security powers has been much debated. It is generally agreed that these powers are and should be extensive. Already in 1990, Koh noted "the president's functional superiority in responding to external events."[325] Goldsmith similarly wrote of "the grim reality of presidential responsibility" over national security."[326] Numerous proposals have been made as to how the law should cabin, channel, and check these executive branch powers to safeguard democracy. This topic becomes especially urgent when the President asserts these powers to oversee data flows in and out of the United States.

One seminal work on the question of executive branch power over foreign affairs is Koh's *The National Security Constitution*.[327] Writing after the Iran-Contra affair of the Reagan administration, Koh calls for "balanced institutional participation."[328] Koh concedes that there is a "predominant

322 *See* Ralls Corp. v. Comm. on Foreign Inv. in U.S., 758 F.3d 296, 312 (D.C. Cir. 2014) (arguing that Ralls's due process challenge to the Presidential Order raises a "non-justiciable political question").

323 See *id.* at 314 (writing that Ralls's due process claim does not encroach on the prerogative of the political branches, does not require the exercise of non-judicial discretion, and is susceptible to judicially manageable standards). *See generally* Marbury v. Madison, 5 U.S. (1 Cranch) 137 (1803).

324 *Id.* at 325.

325 HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION: SHARING POWER AFTER THE IRAN CONTRA AFFAIR 79 (1990).

326 JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11, at 26 (2012).

327 *See generally* KOH, *supra* note 325.

328 *See id.* at 69 (emphasis omitted).

role" for the President in national security, but he argues that the foreign affairs power is, as a matter of constitutional structure, "a *power shared* among the three branches of the national government."[329] For Koh, this vision requires creation by Congress of a new statutory framework, including revisions to IEEPA to limit the President's emergency powers.[330] These reforms are to include requirements that the President make a more extensive showing before declaring a "national emergency" under IEEPA.[331] Ultimately, the result should be fealty to "the principles of shared power and balanced institutional participation in national security decision making."[332]

In his book *Power and Constraint: The Accountable Presidency After 9/11*, Goldsmith offers a different perspective from that offered by Koh. Indeed, Goldsmith argues that as a government official during the Obama administration, Harold Koh did not invariably act consistently with the vision he had laid out as a scholar.[333] It is understandable and usual that Presidents and their advisors take on an institutional perspective, Goldsmith adds, due to the sometimes grim duties associated with protecting national security.[334] At the same time, however, Goldsmith generally welcomes a new development: "[t]he presidential synopticon," a term he uses to describe the large amount of organizations and actors now monitoring presidential actions over national security.[335] These "distributed forces" have worked as a check on the President.[336] The distributed forces include courts, Congress, government lawyers, the media, and human rights organizations, with the result that "the 'many' . . . constantly gaze on the 'one,' the presidency."[337]

In the case of the regulation of international data flows, there are initial indications of interbranch participation in national security decisions, as well as Goldsmith's "presidential synopticon" at work. For example, courts have acted through the litigation that led federal judges to enjoin the Trump administration orders to shut down TikTok and WeChat in the United States.[338] There, we can see Koh's "National Security Constitution" at work.

---

329 *See id*.

330 *See id*. at 196-98 (discussing Koh's proposed revisions).

331 *Id*. at 196.

332 *Id*. at 207.

333 GOLDSMITH, *supra* note 326, at 20-22. Goldsmith quotes Koh in a speech at the American Society of International Law annual meeting as saying, "The making of U.S. foreign policy is infinitely harder than it looks from the ivory tower." *Id*. at 22.

334 *See id*. at 23-24 (providing historical examples of presidents who changed their beliefs on the use of executive power after taking office).

335 *See id*. at 207 ("The various forms of watching and checking the presidency described in this book constitute a vibrant presidential synopticon.").

336 *See id*. at xiii.

337 *Id*.

338 *See* Michael T. Borgia, David M. Gossett, Ambika Kumar, & Thomas R. Burke, *Biden Administration Rescinds Trump's TikTok and WeChat Bans, Issuing Two Executive Orders Highlighting*

But we must also recognize that Congress has delegated a generous amount of authority through FIRRMA to the executive branch and, in particular, CFIUS.[339] And the March 2023 TikTok hearing in the House saw members of Congress outdoing themselves in urging strong executive branch action. Summarizing the feelings of many that day, Representative Randy Weber concluded, "[I]f this committee gets its way, TikTok's time is up."[340] With the enactment of the TikTok Law, CFIUS did indeed get its way.

The limitations on executive power in this statute are surprisingly modest. As part of a determination that a covered company presents "a significant threat to the national security of the United States," the President must issue a public notice proposing this determination and a public report to Congress that includes "a classified annex" as well as a "description of what assets would dneed to be divested to execute a qualified divestitute."[341] The law also limits judicial review to the U.S. Court of Appeals for the DC Circuit.[342]

These few restrictions seem inadequate to stop political calculations in the decision to declare certain applications as national security threats under the TikTok Law. For example, former President Donald Trump surprisingly announced his opposition to the bill that became the TikTok Law, despite having sought to ban this platform or to compel its sale in 2020. On his own social media app, former President Trump argued that TikTok's loss would only benefit its competitor Meta, which had banned him from Facebook for two years in the wake of the January 6, 2021 rioting.[343] Decisions about what apps to allow or ban should not turn on political calculations about which apps are more likely to favor one candidate or another. This development confirms the need for rule of law limitations on executive branch authority over international data flows in the name of national security.

Policies on Chinese Tech Companies, DAVIS WRIGHT TREMAINE LLP (Oct. 26, 2021), https://www.dwt.com/blogs/media-law-monitor/2021/10/biden-tiktok-executive-order#:~:text=In%20June%202021%2C%20President%20Biden,or%20were%20enjoined%20by%20courts [https://perma.cc/G6DB-L3ZE] (noting that the bans "never took effect because they came too late or were enjoined by courts").

339 *See supra* Section I.C.

340 Zachary Basu, *TikTok's Time in the Barrel*, AXIOS (Mar. 23, 2023), https://www.axios.com/2023/03/23/tiktoks-time-in-the-barrel.

341 21st Century Peace Through Strength Act, H.R. 8038, 118th Cong. div. D § 2(g)(3) (2024).

342 *Id*. § 3(b).

343 Edward Helmore, *Donald Trump Flip-Flops on TikTok and Now Rails Against a Ban*, GUARDIAN (Mar, 11, 2024, 7:19 PM), https://www.theguardian.com/technology/2024/mar/11/donald-trump-tiktok-ban-biden.

2. Initial Responses and Future Research

Harold Koh's *National Security Constitution* was crafted against a context of executive overreach in covert operations and disguised money flows.[344] Jack Goldsmith's concept of the Accountable President was devised after watching the Obama Presidency take a measured response to post-9/11 actions of the Bush administration.[345] How might we now update the lessons from these scholars for an era of cross-border flows of data?

The contents of a National Security Constitution for Personal Data remain largely terra nova. Nonetheless, one can sketch three elements necessary to it as well as topics for future research. These three elements should be expressed though a framework statute that would protect free expression and due process when the President acts on national security grounds to control information systems.

First, if the U.S. government is to ban or restrict an information app on national security grounds, it should provide specific evidence of the risks presented by that app to the public. Invocations of threats that are generic to a wide swath of information media, both foreign-owned and in the hands of domestic owners, should generally not be enough. Otherwise, the executive could pick and choose information services to target based on political reasons but disguise its actions as a national security operation. For example, it is likely possible to find a security vulnerability with nearly every app, whether foreign or domestic, large or small.[346] Such a vulnerability might be an intentional back door for a foreign actor, or an accidental and potentially inevitable oversight in a complex program.

Second, there should be judicial process available to test the government's foreign threat claims before an independent tribunal. The statute empowering CFIUS had originally sought to strip courts of any authority to review action taken under it, stating, "The provisions of . . . this section shall not be subject to judicial review."[347] Nonetheless, as we have seen, the D.C. Circuit Court of Appeals allowed a due process challenge to a CFIUS order.[348] The *Ralls* court found that the plaintiffs had a vested, constitutionally protected property right in the companies that it had

344 *See* KOH, *supra* note 325 and accompanying text.

345 *See* GOLDSMITH, *supra* note 326, at 26-27.

346 As an example of a recently discovered major vulnerability in the chips used in Macs, see Dan Goodin, *Unpatchable Vulnerability in Apple Chip Leaks Secret Encryption Keys*, ARS TECHNICA (March 21, 2024, 10:30 AM), https://arstechnica.com/security/2024/03/hackers-can-extract-secret-encryption-keys-from-apples-mac-chips [https://perma.cc/G8CP-XS3S].

347 Defense Production Act of 1950, 50 U.S.C. app. § 2170(e).

348 *See* Ralls Corp. v. Comm. on Foreign Inv. in U.S., 758 F.3d 296, 314 (D.C. Cir. 2014).

acquired.[349] The court would not allow the government to evade judicial review of its order for technical reasons.[350]

While a court is not well-positioned to "second guess" national security judgments, it can certainly review whether the case that the government makes is a sensible one and consider the affected party's response.[351] A new statutory framework should make explicit the availability of such judicial review. Whatever the merits otherwise of the TikTok Law, it did learn the lessons of *Ralls*, as it creates a right of review for any challenge to the act "or any action, finding, or determination under this Act" in the D.C. Circuit.[352]

Third, the government will often argue that it cannot share certain information with the foreign-controlled or foreign-influenced party because this action might compromise its own espionage methods or reveal security vulnerabilities.[353] Lawyers with sufficient security clearances, however, should be available to enable access to information for affected parties to mount a full defense. A related approach is available from a 2015 amendment to the Foreign Intelligence Surveillance Act that granted amicus curiae access to argue before the secret Foreign Intelligence Surveillance Court (FISC).[354] This position, composed of court-appointed experts with security clearances, was introduced in the USA FREEDOM Act in the wake of the Edward Snowden revelations.[355] These experts serve an advisory role within the FISC and "SHALL HAVE Access to any legal precedent, application, certification, petition, motion, or such other materials that the court determines are relevant to the duties of the amicus curiae . . . ."[356]

There is now, in fact, a trend of enhancing justiciability in the national security context. Along with the presence of amicus curiae in the FISC, the Biden administration has established a new redress mechanism to resolve

---

349 *See id.* at 315-17.

350 *See id.* at 321-325 (explaining why the revocation of the CFIUS order impermissibly left a possible wrong to be "capable of repetition yet evading review").

351 *See* Ralls Corp. v. Comm. on Foreign Inv. In U.S., 926 F. Supp. 2d 71, 95 (D.D.C. 2013) (reasoning that a due process claim "raises a pure legal question that can be answered without second-guessing the President's determinations").

352 21st Century Peace Through Strength Act, H.R. 8038, 118th Cong. div. D § 3 (2024).

353 *See* Schaerr v. United States Dep't of Just., 69 F.4th 924, 929 (D.C. Cir. 2023) ("Because withholding national security information is 'a uniquely executive purview,' we exercise great caution before compelling an agency to release such information." (citing Elec. Priv. Info Ctr. v. Nat'l Sec. Agency, 678 F.3d 926, 931 (D.C. Cir. 2012)).

354 *See* EDWARD C. LIU, CONG. RSCH. SERV., R47477, REAUTHORIZATION OF TITLE VII OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 2 (2023).

355 *See* 50 U.S.C. § 1803(I)(1); JASON PYE & SEAN VITKA, *Congress Poised to Jam Through Reauthorization of Mass Surveillance*, HILL (November 30, 2017, 6:20 AM), https://thehill.com/opinion/cybersecurity/361875-congress-poised-to-jam-through-reauthorization-of-mass-surveillance [https://perma.cc/RQX2-632R] (noting the cotemporaneous nature of Title VII's reauthorization and the Snowden leaks).

356 50 U.S.C. § 1803(I)(6).

complaints from any individual whose personal data has been transferred from the European Union to companies in the United States.[357] These individuals can complain about the collection and use of their personal data by U.S. intelligence agencies, and after an investigation by a Civil Liberties Protection Officer in the U.S. Intelligence Committee, individuals have the possibility to appeal the decision of the Officer to a newly created Data Protection Review Court.[358] Adoption of our proposals above, relating to judicial process and information sharing, would continue this trend.

Regarding future research, we have suggestions regarding three areas. Our initial suggestion can be characterized as the issue of "Tit-for-Tat for TikTok." The political and legal scrutiny of TikTok in the United States may already be provoking blowback in China. As an example, there are reports that China has barred employees at governmental agencies and state-owned enterprises from using iPhones at work.[359] These reports at one point caused a nearly 200 billion dollar decline in Apple's market value.[360]

Moreover, Project Texas is an example of a data localization maneuver that may ultimately have repercussions for U.S. tech companies. Regulation in the United States is now creating a strong incentive for foreign companies to store U.S. data in this country. This development will likely encourage additional laws in other countries to adopt new localization measures with the result of a highly problematic balkanization of the Internet.[361] Swire and Sacks argue, moreover, that beyond commercial losses for U.S. tech firms, "localization weakens cooperation with allies by making it more difficult to effectively share data for law enforcement, intelligence, health research, and other common purposes."[362]

As a second issue, localization and pressure on foreign platforms can also generate power for the executive to steer business to favored donors and supporters. One explanation for the choice of Oracle to run TikTok's Project Texas is that it is one of the few tech companies with high-level supporters of then President Donald Trump. These individuals are Larry Ellison, its co-

---

357 *See* Press Release, White House, Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework (Oct. 7, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework [https://perma.cc/C7EL-LFLG].

358 *See id.* (describing the mechanisms created by Executive Order 14086).

359 Mariko Oi & Chris Vallance, *Apple Shares Slide After China Government iPhone Ban Reports*, BBC (Sept. 8, 2023), https://www.bbc.com/news/business-66748092 [https://perma.cc/FK99-UAVS].

360 *Id.*

361 *See generally* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677 (2015) ("The era of a global Internet may be passing.").

362 *See* Swire & Sacks, *supra* note 242.

founder, and Safra Catz, its CEO.[363] Consider as well that the TikTok Law requires the President to determine whether any divestiture was sufficient to avoid foreign control or cooperation.[364] In that light, it is telling that Steven Mnuchin, former Treasury Secretary, has emerged as the leader of a consortium of investors that seeks to purchase TikTok from ByteDance.[365] A decision by a foreign platform to sell to one or another investor might turn on its assessment of whether the purchaser was in favor or disfavor with the current or future President.

Finally, there is the issue of group privacy and free expression. The President's nascent power in this area, supported with congressional enthusiasm, raises potential threats to our nation's long-standing commitment to free expression as well as normative questions about the suitability of a continuing devotion to foreign affairs exceptionalism. There are also special dangers in relying on information privacy law to help sort out these issues.

Daniel Solove and one of the authors of this Article have worried that expanding definitions of personal information might make privacy law unmanageable.[366] Solove and Schwartz explain, "In a world overflowing with information, the law cannot possibly regulate all of it. Yet, without adequate boundaries on regulation, privacy rights would expand to protect a nearly infinite array of information, including practically every piece of statistical or demographic data."[367]

When it comes to First Amendment claims in this area, the government is now asserting the group privacy of users in the United States, who in turn, might defend their own free expression claims in opposing the government's wish to protect their personal information. The resulting thicket of constitutional issues deserves significant further exploration. Should the First Amendment rights of Americans, including companies based in the United States, yield to group privacy claims raised on national security claims? What is the appropriate nature of judicial scrutiny of such claims?

---

363 Chander, *supra* note 138, at 1152-53 (describing the selection of Oracle as TikTok's business partner); *see* Brendan Bordelon, *Trump's TikTok Flip Raises Concerns over Billionaire Clout*, POLITICO (Mar. 14, 2024, 5:00 AM), https://www.politico.com/news/2024/03/14/trump-tiktok-billionaire-donors-00146892.

364 *See* 21st Century Peace Through Strength Act, H.R. 8038, 118th Cong. div. D § 2(g)(6) (2024).

365 Rohan Goswami & Jesse Pound, *Former Treasury Secretary Mnuchin Is Putting Together an Investor Group to Buy TikTok*, CNBC (Mar. 14, 2024, 9:54 AM), https://www.cnbc.com/2024/03/14/former-treasury-secretary-mnuchin-is-putting-together-an-investor-group-to-buy-tiktok.html [https://perma.cc/RR78-3KKD].

366 *See generally* Schwartz & Solove, *supra* note 188.

367 *Id.* at 1866.

CONCLUSION

The laws, executive orders, and regulations under examination in this Article demonstrate that the executive branch effectively asserts the power to erect a Great Firewall of America to protect Americans from foreign data exploitation. There is a good reason for this development: the importance of the digital realm to national security, as evident in a history of government cross-border influence operations, hacking, and spying.[368] A former U.S. Air Force Chief of Staff describes cyberspace as the "fifth operational domain" of conflict—joining land, sea, air, and space.[369]

At the same time, there is reason to be cautious about the immense powers that the executive is asserting in the name of national security. We might recall that the official moniker for what we call the "Great Firewall of China" is the "Golden Shield."[370] Its official purpose is to protect the Chinese people and the Chinese state from foreign adversaries. The Great Firewall of America seems intended to play a similar role. But as the Chinese example shows, such digital defenses can be employed for political purposes. We need to ensure that checks and balances remain vigorous to ensure that the United States does not retreat from its commitment to free expression and due process, even as it protects national security.

---

368 *See, e.g.*, Zizhu Zhang, *Study Confirms Influence of Russian Internet Trolls on 2016 Election*, COLUM. UNIV. SCH. INT'L & PUB. AFFS. (Mar. 29, 2022), https://www.sipa.columbia.edu/news/study-confirms-influence-russian-internet-trolls-2016-election [https://perma.cc/6AWX-5EQ8] (discussing the Russian Internet Research Agency's central role in efforts to interfere in the 2016 United States presidential election); Josh Fruhlinger, *The OPM Hack Explained: Bad Security Practices Meet China's Captain America*, CSO (Feb. 12, 2020), https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html [https://perma.cc/9VQR-3PM5] (attributing the 2015 Office of Personnel Management hack involving the theft of personal information of millions of federal employees to Chinese hackers); Greg Myre, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (Apr. 16, 2021, 10:05 AM), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack [https://perma.cc/K8MV-7GN7] (discussing the cyberattack, attributed to Russian-state actors, that compromised the SolarWinds Orion software and provided attackers with access to thousands of customers data, including many in the U.S. government).

369 GEN. LARRY D. WELCH, INST. FOR DEF. ANALYSES, CYBERSPACE—THE FIFTH OPERATIONAL DOMAIN 2 (2004).

370 Yaqui Wang, *In China, the 'Great Firewall' Is Changing a Generation*, POLITICO (Sept. 1, 2020, 4:30 AM), https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385 (describing the Golden Shield project).

APPENDICES

A. *Executive Orders and Regulations on Cross-border Data Flows*

May 15, 2019	Securing Supply Chains Executive Order 13873 (IEEPA): Trump issues Executive Order on Securing the Information and Communications Technology and Services Supply Chain
Sept. 11, 2019	FIRRMA regulations (CFIUS): Treasury Dept. Office of Investment Security proposes FIRRMA implementation regulations, defining "sensitive personal data"
Aug. 6, 2020	TikTok Ban (IEEPA): Trump issues Executive Order 13942 (TikTok Ban) and Executive Order 13943 (WeChat Ban)
Aug. 14, 2020	TikTok CFIUS Divestiture Order (CFIUS): Trump issues order requiring ByteDance's divestiture of TikTok in the United States
Jan 5., 2021	Alipay Ban (IEEPA): Trump issues Executive Order 13971: Addressing the Threat Posed by Applications . . . Controlled by Chinese Companies
Jan. 21, 2021	ICTS Supply Chain Rule (IEEPA): Commerce Dept. proposes Supply Chain Rule to implement Executive Order 13873
June 9, 2021	Sensitive Data Executive Order 14034 (IEEPA): Biden issues Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries; withdraws app bans
Sept. 15, 2022	Executive Order 14083 (CFIUS): Biden issues Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by CFIUS
Feb. 28, 2024	Data Broker Executive Order 14117 (IEEPA): Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern

B. *OIS Definition of Sensitive Personal Data*[371]

§ 800.241—Sensitive personal data.

(a) The term sensitive personal data means, except as provided in paragraph (b) of this section:

(1) Identifiable data that is:

(i) Maintained or collected by a U.S. business that:

(A) Targets or tailors products or services to any U.S. executive branch agency or military department with intelligence, national security, or homeland security responsibilities, or to personnel and contractors thereof;

(B) Has maintained or collected such data on greater than one million individuals at any point over the preceding twelve (12) months; or

(C) Has a demonstrated business objective to maintain or collect such data on greater than one million individuals and such data is an integrated part of the U.S. business's primary products or services; and

(ii) Within any of the following categories:

(A) Data that could be used to analyze or determine an individual's financial distress or hardship;

(B) The set of data in a consumer report, as defined pursuant to 15 U.S.C. 1681a, unless such data is obtained from a consumer reporting agency for one or more purposes identified in 15 U.S.C. 1681b(a) and such data is not substantially similar to the full contents of a consumer file as defined pursuant to 15 U.S.C. 1681a.;

(C) The set of data in an application for health insurance, long-term care insurance, professional liability insurance, mortgage insurance, or life insurance;

(D) Data relating to the physical, mental, or psychological health condition of an individual;

(E) Non-public electronic communications, including without limitation email, messaging, or chat communications, between or among users of a U.S. business's products or services if a primary purpose of such product or service is to facilitate third-party user communications;

371 Definitions as provided in Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 84 Fed. Reg. 50174, 50189 (Sept. 24, 2019).

> (F) Geolocation data collected using positioning systems, cell phone towers, or WiFi access points such as via a mobile application, vehicle GPS, other onboard mapping tool, or wearable electronic device;
>
> (G) Biometric enrollment data including without limitation facial, voice, retina/iris, and palm/fingerprint templates;
>
> (H) Data stored and processed for generating a state or federal government identification card;
>
> (I) Data concerning U.S. Government personnel security clearance status; or
>
> (J) The set of data in an application for a U.S. Government personnel security clearance or an application for employment in a position of public trust; and

(2) Genetic information, as defined pursuant to 45 C.F.R. 160.103.

(b) The term sensitive personal data shall not include, regardless of the applicability of the criteria described in paragraph (a) of this section:

(1) Data maintained or collected by a U.S. business concerning the employees of that U.S. business, unless the data pertains to employees of U.S. Government contractors who hold U.S. Government personnel security clearances; or

(2) Data that is a matter of public record, such as court records or other government records that are generally available to the public.