NOTE

TIKTOK MIGHT STOP: WHY THE IEEPA CANNOT REGULATE PERSONAL DATA PRIVACY AND THE NEED FOR A COMPREHENSIVE SOLUTION

ALICIA FAISON*

INTRODUCTION

In Spring 2020, as the COVID-19 pandemic shuttered most entertainment outside the home, millions of Americans downloaded their new favorite productivity drain: TikTok. The app, which has accumulated more than 100 million monthly users across the United States,[1] allows users to watch and share 60-second videos on virtually any topic. As they scroll through their homepages, users see videos that reflect their preferences, which are identified by TikTok's algorithm.

Although TikTok purports to "inspire creativity,"[2] some U.S. lawmakers see a much more insidious motive: capture consumers' personal data[3] for use by hostile foreign governments.[4] Because

* J.D. Candidate, Duke Law School, Class of 2022.

1. Alex Sherman, *TikTok Reveals Detailed User Number for the First Time*, CNBC (Aug. 24, 2020), https://www.cnbc.com/2020/08/24/tiktok-reveals-us-global-user-growth-numbers-for-first-time.html.

2. *About TikTok*, TIKTOK, https://www.tiktok.com/about?lang=en (last visited Mar. 5, 2021).

3. "Personal data" or "personal information" has a broad definition. Throughout this Note, I refer to personal data as any information which identifies or could be linked to an individual or their household. *See, e.g.*, *California Consumer Privacy Act (CCPA)*, OFF. OF THE ATT'Y GEN. OF CAL., https://oag.ca.gov/privacy/ccpa (last visited Nov. 3, 2020) ("For example, [personal data] could include your name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.").

4. *See* Jack Nicas et al., *TikTok Said to Be Under National Security Review*, N.Y. TIMES (Nov. 1, 2019), https://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html (describing national security review of Bytedance acquisition of Musical.ly, a TikTok

TikTok's parent company, Bytedance, is based in the People's Republic of China, legislators are concerned that Chinese law compels the platform to share user data with the Chinese government.[5] TikTok concedes that it collects user data, but maintains that the data is held on U.S.-based servers and is not shared with any government officials.[6] Despite TikTok's reassurances, a U.S. Department of Defense memo sent to various military agencies in December 2019 noted a "potential risk associated with the TikTok app" and advised military personnel to delete it.[7]

Interestingly, TikTok uses the same data mining practices as many other companies.[8] The threat TikTok allegedly poses—that, as a Chinese company, it could be compelled to share information with the Chinese government—is shared by many popular gaming platforms.[9] These platforms, which produce widely used video games like Fortnite, are also created by Chinese companies and similarly collect user data.[10] Further, the concerns about TikTok say nothing of the risk that the Chinese government could acquire Americans' personal data by other means, like hacking into U.S. databases or legally buying data from data brokers.[11]

Despite the apparent ordinariness of TikTok's data practices, on August 6, 2020, President Trump issued an executive order banning the app, asserting that TikTok's data mining practices "threaten the

---

precursor); *see also*, Christopher Wray, Dir., Fed. Bureau of Investigation, Address at the Hudson Institute: The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States (July 7, 2020) ("The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security—and by extension, to our national security.").

5. Letter from Sen. Charles E. Schumer & Sen. Tom Cotton to Joseph Maguire, Acting Dir. of National Intelligence (Oct. 23, 2019) (on file with United States Senate).

6. *See Privacy Policy*, TIKTOK, https://www.tiktok.com/legal/privacy-policy?lang=en (last updated Dec. 20, 2020) (explaining that Tiktok collects usage information, device information, location data, messages, metadata, and cookies).

7. Neil Vigdor, *U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning*, N.Y. TIMES (Jan. 4, 2020), https://www.nytimes.com/2020/01/04/us/tiktok-pentagon-military-ban.html.

8. Keman Huang & Stuart Madnick, *The TikTok Ban Should Worry Every Company*, HARV. BUS. REV. (Aug. 28, 2020), https://hbr.org/2020/08/the-tiktok-ban-should-worry-every-company.

9. Aynne Kokas, *China Already Has Your Data. Trump's Tiktok and Wechat Bans Can't Stop That.*, WASH. POST (Aug. 11, 2020), https://www.washingtonpost.com/outlook/2020/08/11/tiktok-wechat-bans-ineffective/.

10. *Id.*

11. *See infra* Part II.

national security, foreign policy, and economy of the United States."[12] Since the announcement was made, the move has been harshly criticized as a political distraction that infringes on the First Amendment rights of TikTok's users,[13] and alternatively, praised for confronting Chinese data collection tactics.[14] Whether a ban will actually take effect is a different question, as the Biden Administration indicated it might drop the issue entirely.[15]

Although TikTok is the cybersecurity[16] controversy de rigueur, the debate about its data mining practices reflects more fundamental questions about the governance of our personal data: Is personal data privacy truly a national security concern? If so, how should we regulate it?

Ineffective personal data privacy regulation poses a grave national security risk—namely, that our data could be misused by hostile actors. However, protection of personal data cannot be successfully implemented through ad hoc maneuvering like the TikTok ban. Instead, effective protection requires comprehensive legislation that addresses what data is allowed to be collected, and what companies can do with it.

Although President Trump seemed to agree that personal data security is of paramount concern, his approach to addressing the issue is ultimately untenable.[17] In imposing the ban on TikTok, the President's Executive Order cited to powers granted under the

12. Exec. Order No. 13942, 85 Fed. Reg. 48,637 (Aug. 11, 2020).

13. Mike Isaac & David McCabe, *TikTok Wins Repreive from U.S. Ban*, N.Y. TIMES (Sept. 27, 2020), https://www.nytimes.com/2020/09/27/technology/tiktok-ban-ruling-app.html.

14. James Jay Carafono, *Why Trump's TikTok Battle With China Is Worth Fighting*, HERITAGE FOUND. (Aug. 6, 2020), https://www.heritage.org/cybersecurity/commentary/why-trumps-tiktok-battle-china-worth-fighting.

15. *See* Unopposed Motion to Hold Appeal in Abeyance at 2, Marland v. Trump, No. 20-4597, 2020 U.S. Dist. LEXIS 202572, at *38–39 (E.D. Pa. Oct. 30, 2020), *appeal docketed sub nom* Marland v. Biden, No. 20-3322 (3d Cir. Feb. 10, 2021) (The Department of Justice moved to stay the case pending in the Third Circuit after the Trump Administration's claims were dismissed and appealed); *see also* Tiktok Inc. v. Trump, No. 1:20-cv-02658, 2020 U.S. Dist. LEXIS 177250, at *3 (D.D.C. Sept. 27, 2020) (dismissing the Trump Administration's case against TikTok).

16. By "cybersecurity," I refer broadly to the frameworks that protect data. *See also* Dan Craigen et al., *Defining Cybersecurity*, 4 TECH. INNOVATION MGMT. REV. 13, 13 (discussing various definitions of cybersecurity).

17. *See* Donald J. Trump (@realdonaldtrump), TWITTER (Aug. 23, 2019, 11:58 AM), https://www.thetrumparchive.com/?dates=%5B%222019-08-23%22%2C%222019-08-24%22%5D ("For all the Fake News Reporters that don't have a clue as to what the law is relative to Presidential powers, China, etc., try looking at the Emergency Economic Powers Act of 1977. Case closed!").

International Emergency Economic Powers Act of 1977 (IEEPA).[18] The IEEPA empowers the President to impose economic sanctions to confront "any unusual or extraordinary threat" to national security that has its origins outside the U.S.[19] The President may exercise these powers after he declares a national emergency in accordance with the National Emergencies Act (NEA).[20]

Congress originally enacted the IEEPA to provide a check on executive power.[21] In doing so, Congress defined three limitations on the President's authority. First, the powers under the statute may only be invoked during times of national emergency.[22] According to a House Report on the IEEPA, national emergencies are "rare and brief, and are not to be equated with normal ongoing problems."[23] The second limitation gave Congress the power to review and terminate the national emergency.[24] Congress was to meet every six months to discuss whether to veto the President's executive order declaring emergency.[25] The third constraint precluded regulation of "personal communications" or "informational materials" under the IEEPA,[26] which include films, photographs, CD-ROMs, etc.[27]

Despite these efforts to limit executive power, the IEEPA is now being used contrary to its legislative intent. Over time, Presidents have used IEEPA powers expansively and with greater frequency to further foreign policy objectives.[28] Further, Supreme Court decisions

18. Exec. Order No. 13942, 85 Fed. Reg. 48,637 (Aug. 11, 2020).

19. International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–08 (2018).

20. National Emergencies Act, 50 U.S.C. §§ 1601–51 (2018).

21. CHRISTOPER A. CASEY ET AL., CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE 6–9 (2020).

22. 50 U.S.C. § 1701(b).

23. H.R. REP. NO. 95-459, at 10 (1977).

24. 50 U.S.C. § 1706(b).

25. 50 U.S.C. § 1706(d); *see also* Harold H. Koh, *Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the Iran Contra Affair*, 97 YALE L.J. 1255, 1264 (1988) ("Congress drafted IEEPA specifically to narrow the President's authority in nonwartime situations, conditioning his exercise of emergency powers upon prior congressional consultation, subsequent review, and legislative veto termination provisions.").

26. 50 U.S.C. § 1702(b).

27. *Id.*

28. CASEY ET AL., *supra* note 21, at 17; *see also id.* at 52–53, 60–63 (comparing President Reagan's declaration of four national emergencies to President Obama's eleven throughout their respective presidency); *see also* Gregory Korte, *White House: States of Emergency are Just Formalities*, USA TODAY (Apr. 9, 2015), https://www.usatoday.com/story/news/politics/2015/04/09/pro-forma-states-of-national-emergency/25479553/ (noting that after President Obama froze Venezuelan assets under the IEEPA, the administration later admitted that Venezuela did not pose a threat to the U.S. at all, and the national emergency declaration was merely a formality).

undermined Congress's oversight mechanisms and declared the legislative veto invalid.[29] The Court upheld the President's broad authority under the IEEPA,[30] reflecting the well-established belief that foreign affairs are primarily the province of the executive branch.[31]

In banning TikTok under the IEEPA, the Trump Administration evinces an overreach of executive power—the kind that the IEEPA intended to prevent. Indeed, it seems odd that the IEEPA could be invoked to oppose foreign adversaries that are "*increasingly* creating and exploiting vulnerabilities in information and communications technology and services . . . in order to commit . . . economic and industrial espionage against the United States and its people."[32] By the Trump Administration's own definition, then, the security issues posed by TikTok are neither rare nor brief.[33]

Therefore, it is invalid to use the IEEPA to regulate threats to Americans' personal data. First, these risks are not extraordinary national emergencies at all. Instead, these are known, widespread national security threats that require more comprehensive solutions. Second, the ban on TikTok violates the IEEPA carve-out on informational materials. Finally, given the extensiveness of the personal data security risk, Congress should have a greater role in regulation than an IEEPA framework would allow. Accordingly, this Note argues that personal data security cannot be adequately regulated through the framework mandated by the IEEPA, and instead requires a broad, long-term solution.

Part I will survey prior efforts to address personal data privacy in the U.S. to show how inattention to the risks posed by personal data collection created a fractured privacy framework ripe for exploitation. Part II will examine the widespread risks inherent in the personal data marketplace and will demonstrate the need for an ongoing resolution

29. *See generally* Regan v. Wald, 468 U.S. 222 (1984) (upholding use of emergency powers against Cuba pursuant to the IEEPA); *see also* INS v. Chadha, 462 U.S. 919 (1983) (invalidating the legislative veto); *see also* Dames & Moore v. Regan, 453 U.S. 654 (1981) (giving broad interpretation to the President's IEEPA authorities).

30. *Dames & Moore*, 453 U.S. at 678 (quoting Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 637 (1952) (Jackson, J., concurring)).

31. *See* Koh, *supra* note 25, at 1305 ("Whether on the merits or on justiciability grounds, the courts
have held for the President in [foreign affairs] cases with astonishing regularity.").

32. Exec. Order No. 13873, 84 Fed. Reg. 22,689 (May 17, 2019) (emphasis added).

33. *See* Defendants' Memorandum in Opposition to Plaintiffs' Motion for a Preliminary Injunction at 5, TikTok Inc. v. Trump, No. 1:20-CV-2658-CJN (D.D.C. Sept. 25, 2020) (describing China as a "persistent" and "growing" threat).

to those national security threats. Part III will argue that application of the IEEPA is inappropriate to regulate personal data privacy; the statute is not designed to bear on events that are not a "state of emergency," exempts personal communications and informational materials from its reach, and improperly limits Congress's role. Part IV will suggest that comprehensive congressional legislation is needed, and looks to California's Data Privacy legislation as a model for a federal data protection law.

I. PATCHWORK PROTECTION: DATA PRIVACY IN THE UNITED STATES

This Part provides an overview of the security risks posed by inadequate personal data protection law. However, it is important to first understand the existing data privacy framework in the United States. This Part begins by surveying the judicial approach to privacy and the patchwork of federal data protection legislation. Prior administrations' cybersecurity efforts misunderstood the scope of the national security problem, leaving significant gaps in the protection of our personal data. Partially as a result of the U.S. government's response, inadequate data protection policy continues to pose the risk that our personal data may be used to benefit our adversaries. Cambridge Analytica's interference in the 2016 election exemplified this danger.

A. U.S. Data Privacy: Judicial Interpretation and Federal Legislative Framework

Neither the courts nor Congress have created robust privacy protection in the United States. Unlike the courts of other countries, the U.S. Supreme Court has declined to recognize an informational privacy right in the Constitution,[34] affording constitutional protection only to privacy invasions by the *government*, rather than by private, hostile actors.[35] Some judicial theorists believe that a constitutional right to informational privacy does not exist in any context.[36]

To the extent an informational privacy right might exist in the U.S.,

34. *See* STEPHEN P. MULLIGAN ET AL., CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 5 (2019) (citing Katz v. United States, 389 U.S. 347, 353 (1967)) (noting that the Fourth Amendment is not read to protect a "general" right to privacy).

35. *Id.*

36. *See* NASA v. Nelson, 562 U.S. 134, 160 (2011) (Scalia, J., concurring) ("A federal constitutional right to 'informational privacy' does not exist.").

it only extends to criminal law. In *Carpenter v. United States*, the Supreme Court determined whether police could use location tracking records from a suspect's cell phone without a warrant.[37] The Court concluded that the Fourth Amendment protects a reasonable expectation of privacy, and allowing government access to location tracking data "contravenes that expectation."[38] Although *Carpenter* acknowledges a distinction between privacy in a digital context and traditional forms of privacy, the Court's relative indifference to informational privacy has changed little in the digital age.

Congress has enacted a limited number of personal informational privacy measures, creating a discordant patchwork of protections that leave significant areas unregulated.[39] Only a few major pieces of legislation actually impose data protection requirements on database operators, in addition to requiring consumer consent for sharing data. Of note, the Communications Act of 1934, and its amendments in 1996, impose data security requirements on "common carriers," namely, telephone services, cable operators and satellite carriers.[40] The Graham-Leach-Bliley Act (GLBA) imposes obligations on financial institutions to protect consumer personal information.[41] Similarly, the Health Insurance Portability and Accountability Act (HIPAA) requires health care providers to protect patients' personal health information and adopt privacy standards.[42] However, these measures have been criticized for offering too many loopholes that allow dissemination of personal information to third parties by record-keepers.[43] Other legislation, like the Fair Credit Reporting Act, does not impose any restrictions on the maintenance of information, but rather imposes only consumer disclosure requirements.[44]

The agencies tasked with enforcement of these provisions, the

37. Carpenter v. United States, 138 S. Ct. 2206, 2212, 2216 (2018).

38. *Id.* at 2217.

39. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014) ("The statutory law regulating privacy is diffuse and discordant . . . . This sectoral approach also leaves large areas unregulated . . . .").

40. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified in scattered sections of 47 U.S.C.); 47 U.S.C. § 153(51).

41. Graham-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2018).

42. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29, and 42 U.S.C.).

43. *See* R. Bradley McMahon, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America*, 49 VILL. L. REV. 625, 651 (2004) ("Both laws, however,
contain loopholes that allow entities to disseminate personal information.").

44. Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2018).

Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB), enjoy broad discretion to implement these requirements.[45] But the fact remains that most U.S. citizens have little control over what personal data is collected, who can access their data, and how third parties can use it.[46]

B. Presidential Efforts to Address Cybersecurity

This piecemeal legislation makes more sense when considered against the backdrop of the federal government's slow acceptance of the cybersecurity risk. In particular, the government's failure to recognize the danger of inadequate protection of *personal*, rather than governmental, data led to the data security incidents we see today.

In 1996, President Clinton enacted Executive Order 13,010, titled Critical Infrastructure Protection.[47] This Order was one of the first national acknowledgements of a "cyber threat," defined as a "computer-based attack[] on the information or communications components that control critical infrastructures."[48] E.O. 13,010 established a commission to report on and recommend resolutions to cyber threats on governmental data.[49] Although the Clinton Administration did not address personal data beyond the enactment of the GLBA and HIPPA, President Clinton's efforts were not without some benefit. Importantly, the Clinton Administration classified the cyber threat as a national security issue, of the same importance as a physical attack. Recognition of these national security implications encouraged subsequent administrations to prioritize the issue.

Initially, the Bush Administration seemed poised to continue building on the Clinton's Administration's cyber framework, but 9/11 changed everything. Where the Clinton Administration believed the cyber threat could be as serious as a physical attack, after 9/11 the Bush Administration, unsurprisingly, refocused national security policy on physical threats.[50] As a result, the Bush Administration's efforts to

45. *See* MULLIGAN, *supra* note 34, at 30, 35 (noting that the FTC covers a "broad range" of activity and the CFPB may take "any" action to prevent covered entities from engaging in deceptive practices).

46. *See id.* at 55 (proposed legislation may afford citizens the legal right to "control the use and dissemination of personal data . . . [and require companies to define] how data is disseminated or disclosed to third parties").

47. Exec. Order No. 13010, 61 Fed. Reg. 37347 (Jul. 15, 1996).

48. *Id.*

49. *Id.*

50. Kevin P. Newmeyer, *Who Should Lead U.S. Cybersecurity Efforts?*, 3 PRISM 115, 117 (2012).

regulate personal data security were minimal in comparison to its broader national security efforts.

Nonetheless, the Bush Administration did implement some data security policies. In 2003, it issued a report titled the *National Strategy to Secure Cyberspace*.[51] The report identified cybersecurity as a key national security issue but still recommended that the federal government take a backseat to private efforts: "[F]ederal regulation will not become a primary means of securing cyberspace . . . the market itself is expected to provide the major impetus to improve cybersecurity."[52] Additionally, in 2008, the Bush Administration established the Comprehensive National Cybersecurity Initiative (CNCI), a set of projects which aimed to reduce online security vulnerabilities, protect against intrusions, and anticipate future cyber-attacks.[53]

Neither of those efforts proved sufficient. The 2003 Report dangerously mischaracterized the proper role of the national government by yielding control of the issue to private companies. As critics of the 2003 Report realized, in no other area of national security does the government rely almost exclusively on market forces or private efforts.[54] In turn, the 2008 CNCI went too far in the other direction—it was heavily classified and its only focus was on protection of government data (".gov" protection).[55]

The Obama Administration, on the other hand, prioritized data privacy as a national security issue. The administration expanded the focus of federal privacy protection, encompassing not just governmental security, but personal data security as well. Almost immediately after taking office, President Obama implemented a sixty-day review of U.S. cybersecurity policy.[56] The review culminated in a

51. WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 15 (2003), *available at* https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.

52. *Id.*

53. JOHN ROLLINS & ANNA C. HENNING, CONG. RSCH. SERV., R40427, COMPREHENSIVE NAT'L CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS 1 (2009).

54. *See* CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY: REP. OF THE CSIS COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY 50 (2008) ("In pursuing the laudable goal of avoiding overregulation, the strategy essentially abandoned cyber defense to ad hoc market forces. . . . In no other area of national security do we depend on private, voluntary efforts.").

55. *See id.* at 15 ("The CNCI has its focus on defending government—.gov, in other words—an approach that skilled opponents will be able to outflank.").

56. FED'N OF AM. SCIENTISTS, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE iii (2009), *available at*

ten-point action plan to strengthen federal policy for both personal and governmental protection.[57] During President Obama's time in office, the administration delivered on most of the goals of the action plan. First, President Obama tasked a cybersecurity czar, Howard Schmidt, with developing a national cyber policy.[58] The Obama Administration improved coordination among federal agencies, delineating the appropriate roles for the DHS, the FBI, and the Office of the Director of National Intelligence in the wake of a cyber-attack.[59] The National Institute of Standards and Technology (a division of the Department of Commerce) improved public-private cybersecurity relationships by developing industry-best practices for cybersecurity management, which were widely implemented by the private sector.[60]

Despite these steps forward, the Obama Administration failed to implement the comprehensive personal data privacy policy they had envisioned. The centerpiece of the Obama Administration's data privacy legislation, a Consumer Privacy Bill of Rights, did not gain traction in Congress. Unlike the Bush Administration's efforts, the Privacy Bill of Rights posited that consumer privacy was a fundamental right that could not be left in the hands of industry.[61] The proposal was nevertheless decried by privacy advocates as insufficient. Conversely, technology companies characterized it as unduly burdensome.[62]

President Obama's term ended shortly after an unprecedented cyber intrusion on one of our nation's most vital institutions: fair and free elections. In 2010, Facebook launched OpenGraph, a service that

---

https://fas.org/irp/eprint/cyber-review.pdf.

57. *Id.* at vi.

58. Larry Greenmeier, *Obama Chooses Howard Schmidt to Coordinate National Cybersecurity*, SCI. AM. (Dec. 22, 2009), https://blogs.scientificamerican.com/observations/obama-chooses-howard-schmidt-to-coordinate-national-cybersecurity/.

59. Travis D. Howard & Jose de Arimateia da Cruz, *Stay the Course: Why Trump Must Build on Obama's Cybersecurity Policy*, 26 INFO. SEC. J.: A GLOBAL PERSPECTIVE 276, 277 (2017).

60. *See id*. For example, NIST recommended a five-step framework for responding to cyber incidents—Identify, Protect, Detect, Respond, Recover. NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 4 (2014), *available at* https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

61. *See* WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT (2015) ("The Congress finds that . . . Americans cherish privacy as an element of their individual freedom.").

62. Brendan Sasso, *Obama's 'Privacy Bill of Rights' Gets Bashed from All Sides*, ATLANTIC (Feb. 27, 2015), https://www.theatlantic.com/politics/archive/2015/02/obamas-privacy-bill-of-rights-gets-bashed-from-all-sides/456576/.

allowed external app developers to reach out to Facebook users for access to their—and crucially, their Facebook *friends'*—personal information.[63] In 2013, the research company GlobalScienceResearch, in collaboration with political consulting firm Cambridge Analytica, created an app that prompted users to answer questions for a psychological profile.[64] By participating, a user gave Cambridge Analytica access to her *and* her friends' personal information.[65] Although Facebook removed OpenGraph's access to friends' data in 2014, the rule did not apply retroactively.[66] So, from an initial 270,000 people who took the quiz, Cambridge Analytica amassed data on 87 million Facebook profiles.[67] In 2016, Cambridge Analytica passed that data to the presidential campaigns of Donald Trump and Ted Cruz, which allegedly used the data to develop intensive voter profiles and target political advertisements to Facebook users.[68] Cambridge Analytica may have also passed data to Russia, which interfered in the general election in favor of President Trump.[69]

The Cambridge Analytica scandal, more than anything, epitomizes the dangers of inadequate personal data protections. Although hacking of government systems may be a real threat, prior administrations' singular focus on that issue demonstrates a failure to understand the breadth of the national security problem. Efforts like the Obama Administration's Consumer Privacy Bill of Rights would have ultimately permitted tech companies to take whatever data they wanted, but imposed restrictions on its distribution.[70] Thus, even

63. *See* Sam Meredith, *Facebook-Cambridge Analytica: A Timeline of the Data Hijacking Scandal*, CNBC (Apr. 10, 2018), https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html ("If accepted, these apps would then have access to a user's name, gender, location, birthday, education, political preferences, relationship status, religious views, online chat status and more. In fact, with additional permissions, external sites could also gain access to a person's private messages.").

64. *Id.*

65. *Id.*

66. *Id.*

67. Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html; Cecilia Kang & Sheera Frankel, *Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html.

68. *Id.*

69. Danny Hakim & Matthew Rosenberg, *Data Firm Tied to Trump Campaign Talked Business with Russians*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-russia.html.

70. *See* Sasso, *supra* note 62 ("Instead, companies and industry associations would write their own rules and then ask the FTC to sign off on them.").

measures specifically meant to protect personal data failed to target the real problem: Allowing expansive data mining increases the risk that data will be used to benefit our adversaries.

II. TIKTOK IS NOT UNIQUE: PERVASIVE THREATS POSED BY THE MARKETPLACE FOR PERSONAL DATA

Although the United States recognized early on that cybersecurity could become a major national security issue and instituted policies protecting *governmental* data, policymakers failed to appreciate the risk created by personal data mining. Thus, personal data security efforts to date have been inadequate.[71]

This brings us back to TikTok. Although TikTok is accused of mining personal data for the benefit of the Chinese government, the national security risk that TikTok poses—that Americans' personal data can end up in the hands of a foreign government—is hardly unique to TikTok.[72] Thus, this Part will describe how the marketplace for personal data creates ongoing cyber threats that cannot be ameliorated by banning one company outright, because hostile actors can acquire data in other ways.

Generally, there are three ways that personal data could be acquired by a foreign government. First is the accusation levied against TikTok: that any foreign company requesting personal data could be compelled to give that data to their government. Second, systems storing personal data could be hacked. Finally, some companies could be selling personal data to hostile actors.

No matter how it is acquired, Americans' personal data in the possession of a hostile foreign government poses a threat to our national security. There are many specific consequences of hostile actors' acquisition of personal data, including the spread of propaganda in an effort to influence American elections and use of personal data to extort, blackmail, and even recruit U.S. citizens to share confidential government information. These consequences demonstrate why protecting our personal data demands a comprehensive national solution.

---

71. *See* SUSAN A. AARONSON, DATA IS DANGEROUS: COMPARING THE RISKS THAT THE UNITED STATES, CANADA, AND GERMANY SEE IN DATA TROVES 8 (2020) ("[N]etizens of the United States have little recourse to ensure that their personal data does not put them or their fellow Americans at risk.").

72. Graham Webster, *The Risks TikTok Poses Are Not At All Unique to TikTok*, SLATE (Aug. 3, 2020), https://slate.com/technology/2020/08/tiktok-ban-microsoft-trump-china-risk.html.

A. TikTok and Other Companies Can Be Compelled to Share Data

The fear that TikTok or other foreign-based companies operating in the U.S. could be compelled to pass off users' data to China or elsewhere is legitimate.[73] For example, China's Cybersecurity Law requires Chinese companies to "provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[74] Although what constitutes compliance is unclear and often results in protracted negotiations, the fact remains that the Chinese government can acquire effectively any information it wants.[75] Likewise, apps developed in Russia pose the same threat.[76]

B. Collection of Personal Data and Risk of Hack

The risks associated with foreign governments compelling access to data, however, presents only a small portion of the overarching personal data security concern. The real threat resides in the mass collection of personal consumer information—known today as "big data."

To understand the ubiquity of technology companies' data mining practices, it is important to understand the personal data marketplace. Personal data refers to the mass of data about an individual that different technologies collect every day. For example, Facebook collects user data not only from an indvidual's Facebook activity, but also through partnerships with other major technology companies, such as Spotify, Netflix, Amazon, etc.[77] The result is a nearly symbiotic relationship: Facebook collects data from Amazon using cookies, which informs how Facebook presents information to users, which, in turn, informs Amazon's targeted advertising strategy for a given user.[78] In

73. *See Dangerous Partners: Big Tech & Beijng: Hearing Before the Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 116th Cong. 2 (2020) (statement of Samm Sacks, Senior Fellow, Yale Law School's Paul Tsai China Center) ("[T]he way Chinese companies handle U.S. citizen data does impact U.S. national security.").

74. *Id.* at 4.

75. *Id.* at 7.

76. *See* Letter from Jill C. Tyson, Assistant Director, Office of Congressional Affairs, Federal Bureau of Investigation to Sen. Charles E. Schumer (Nov. 25, 2019) (on file with United States Senate) ("The FBI considers any mobile application or similar product developed in Russia, such as FaceApp, to be a potential counterintelligence threat . . . .")

77. *See* Gabriel J.X. Dance et al., *As Facebook Raised a Privacy Wall, it Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (reporting that Facebook allowed technology companies expansive access to user data).

78. *Id.*

general, technology companies use this collection of personal data to create a more personalized user experience.

These scraps of data are oftentimes packaged and resold by data brokers, which are companies that aggregate users' personal data to build a composite of their lives.[79] Data brokers collect information from publicly available sources (e.g., property records), social media, other data brokers and commercial sources,[80] and then build profiles based on that data, categorizing those profiles into different segments.[81] As an FTC Report detailed

> [I]n developing their products, the data brokers use not only the raw data they obtain from these sources, such as a person's name, address, home ownership status, or age, but also certain derived data, which they infer about consumers. For example, a data broker might infer that an individual with a boating license has an interest in boating, that a consumer has a technology interest based on the purchase of a "Wired" magazine subscription, or that a consumer who has bought two Ford cars has loyalty to that brand.[82]

These inferences are then used to package consumer information for marketing, risk mitigation and people-search products.[83] Data brokers collect and store information on nearly every American household and the industry is estimated to be worth $200 billion.[84] Whether we know it or not, data brokers are keeping tabs on all of us.

This mass data collection creates the inherent risk that these systems, maintained by data brokers and other companies, could be hacked by a foreign state actor. The consequences of a data breach are severe: In 2017, Equifax, a credit-reporting agency that also functions as

---

79. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY iv (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

80. *Id.* at 11–15.

81. *Id.* at 19.

82. *Id.*

83. *See id.* at 23. "Risk mitigation" refers to fraud detection products. For example, a risk mitigation product might flag a customer using a fraudulent social security to apply for a credit card. "People search products" are tools consumers might use to conduct a search on, for example, a particular person or address. Popular providers include Spokeo and ZoomInfo. *See* Steven Melendez & Alex Pasternack, *Here Are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST CO. (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information (discussing data broker products).

84. Matthew Crain, *The Limits of Transparency: Data Brokers and Commodification*, 20 NEW MEDIA & SOC'Y 88, 90 (2018).

one of the country's largest data brokers, was hacked, exposing the data of 145 million Americans.[85] Four members of China's military were later indicted for the hacking.[86] Equifax was just one example of the growing use of data hacks. As attack technology advances, foreign nations leverage their expertise and resources to gain advantage over U.S. systems.[87] The statistics corroborate the increasing ease of hacks: The number of data breaches grows every year,[88] and since the beginning of 2010, there have been an estimated 40,650 personal data hacks.[89]

One might reasonably think that these companies could impose cybersecurity measures sufficient to guard against a data breach. However, some mistakes cannot be mitigated by even the best cybersecurity infrastructure. Human error, like failing to install a security patch, can open the door to a mass data breach that affects millions.[90] So long as companies continue to collect and store personal data, the risk of a hack will persist.

C. Selling Data and the Risk of Sales to Foreign Governments

The sale of personal data is another major risk about which consumers are often unaware.[91] Consider, for example, the consequences of sending a vial of saliva to 23andMe, a DNA processing service. When 23andMe users click "I DO CONSENT" at the bottom of the company privacy policy, as do 80 percent of 23andMe's customer base, they permit GlaxoSmithKline, a pharmaceutical manufacturer, to view the information gleaned from their saliva and to use that data in

85. Katie Benner, *U.S. Charges Chinese Military Officers in 2017 Equifax Hacking*, N.Y. TIMES (Feb. 10, 2020), https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html.

86. *Id.*

87. U.S. GOV'T ACCOUNTABILITY OFF., GAO-18-622, HIGH RISK SERIES: URGENT ACTIONS ARE NEEDED TO ADDRESS CYBERSECURITY CHALLENGES FACING THE NATION 1, 2 (2018), https://www.gao.gov/assets/700/694355.pdf (noting that "rapid developments in new technologies" have given sophisticated foreign nations the expertise needed to impose "increasing risks").

88. Chris Morris, *Hackers Had a Banner Year in 2019*, FORTUNE (Jan. 28, 2020), https://fortune.com/2020/01/28/2019-data-breach-increases-hackers/.

89. Megan Leonhardt, *The 10 Biggest Data Hacks of the Decade*, CNBC (Dec. 27, 2019), https://www.cnbc.com/2019/12/23/the-10-biggest-data-hacks-of-the-decade.html.

90. *See* Benner, *supra* note 85 (noting that the Equifax hack was due to a failure to install a security patch).

91. *See Your Data Is Shared and Sold. . .What's Being Done About It?*, KNOWLEDGE@WHARTON (Oct. 29, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/# (stating that "[u]p to 73% of American adults incorrectly believe that the existence of a privacy policy means a website cannot share their data with other parties without their permission").

drug development.[92]

Although 23andMe discloses where your data ends up, data brokers do not.[93] Thus, in the context of personal data sales, data brokers are particularly risky. Data brokers are different from something like Facebook, which encounters a certain amount of scrutiny because of its notoriety and size. In contrast, data brokers operate in the shadows—they collect data without consumer knowledge, make inferences about the data, and sell the data to largely unknown customers.[94] Although some data brokers screen their customers to ensure above-the-board data use, there is no law defining who can and cannot buy these mass collections of data.[95]

This lack of transparency means that hostile actors could purchase personal information from data brokers. Recent history shows these security concerns are well-founded. In 2014, the data broker LeapLab bought payday loan applications that included consumers' names, addresses, phone numbers, employers, Social Security numbers, and bank account numbers.[96] LeapLab sold that information to Ideal Financial Solutions, which used the consumer information to make millions of dollars in phony purchases.[97]

If there is no regulatory mechanism preventing personal data sales to Ideal Financial, there is certainly nothing stopping the Chinese government, or any other foreign government for that matter, from buying Americans' data through data brokers.[98] In that sense, there is no material difference between sharing data under foreign national security law and buying it on the open market.

---

92. *See* Megan Molteni, *23andMe's Pharma Deals Have Been the Plan All Along*, WIRED (Aug. 3, 2018), https://www.wired.com/story/23andme-glaxosmithkline-pharma-deal/ (describing how 23andMe develops biological insights from a customer's saliva, such as predisposition to disease, which is then passed on to GlaxoSmithKline to determine targets for drug development).

93. *See Crain*, *supra* note 84, at 91 (describing the information asymmetry between a general public that is "increasingly [subject to] extensive forms of monitoring" and the "institutions doing the monitoring [that remain] hidden from view").

94. *Id.*

95. FED. TRADE COMM'N, *supra* note 79, at 40–41.

96. FTC v. Ideal Fin. Sols., Inc., No. 2:13-cv-00143-JAD-GWF, 2015 U.S. Dist. LEXIS 86348, at *9 (D. Nev. June 29, 2015).

97. *Id.*

98. *See* Dymples Leong & Teo-Yi-Ling, *Data Brokers: A Weak Link in National Security*, THE DIPLOMAT (Aug. 21, 2020), https://thediplomat.com/2020/08/data-brokers-a-weak-link-in-national-security/ ("American companies can still sell data to third-party data brokers, even after buying ownership of foreign-based apps. Those brokers could then turn around and sell the data to the Chinese government.").

D. The Consequences of Data Acquisition

To some, the fact that foreign governments can easily acquire Americans' personal data is self-evidently terrifying. Others might ask, "so what?" Although foreign actors' goals in harvesting American data may not be entirely clear at first, recent history provides some answers.

First, as discussed in Part I, personal data could be used to infiltrate and corrupt American elections through the spread of disinformation.[99] By combining different sets of data, Cambridge Analytica researchers developed a method to "microtarget" individuals, allowing them, for example, to identify people "vulnerable to [extremist] messaging—people who were more prone to conspiratorial thinking or paranoid ideation" and could be convinced to join the alt-right.[100] The targeted individuals often spread their misinformed beliefs across social media channels, effectively creating a self-perpetuating propaganda machine.[101] Since 2016, microtargeting has become one prong[102] in vast campaigns to spread disinformation on social media by countries like Venezuela, Bangladesh, Iran, Russia and China.[103]

Second, personal data can be used to identify and recruit U.S. dissidents to serve as informants for foreign governments.[104] After major data breaches at Equifax, the Office of Personnel Management, and Marriott were linked to the Chinese government, many in the cyber intelligence community concluded that the Chinese were building a database on U.S. citizens.[105] Recent scholarship contends that one purpose of this database is to target persons of interest who have

---

99. *See supra* Part I(B).

100. Terry Gross, *Fresh Air: Whistleblower Explains How Cambridge Analytica Helped Fuel U.S. 'Insurgency,'* NPR (Oct. 9, 2019), https://www.npr.org/2019/10/08/768216311/whistleblower-explains-how-cambridge-analytica-helped-fuel-u-s-insurgency (describing how Cambridge Analytica targeted "people prone to conspiratorial thinking" in disinformation campaigns).

101. *Id.*

102. Other methods include bots and trolls. *See.*, *e.g*, *How is Fake News Spread? Bots, People Like You, Trolls and Microtargeting*, CENTER FOR INFO. TECH. & SOC., https://www.cits.ucsb.edu/fake-news/spread.

103. Sheera Frenkel et al., *Russia's Playbook for Social Media Disinformation Has Gone Global*, N.Y. TIMES (Jan. 31, 2019), https://www.nytimes.com/2019/01/31/technology/twitter-disinformation-united-states-russia.html (describing the growing use of microtargeting techniques to spread disinformation in the U.S. and other countries); Kate Conger, *Facebook and Twitter Say China Is Spreading Disinfomation in Hong Kong*, N.Y. TIMES (Aug. 19, 2019), https://www.nytimes.com/2019/08/19/technology/hong-kong-protests-china-disinformation-facebook-twitter.html.

104. Ming S. Chen, *China's Data Collection on US Citizens: Implications, Risks, and Solutions*, 15 J. OF SCI. P. & GOVERNANCE 1, 1 (2019).

105. Charles J. Dunlap Jr., *The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict*, 15 GEO. J OF INT'L AFF. 108, 110 (2014).

access to confidential governmental information, and could be persuaded or blackmailed to spy on the U.S. government.[106]

Collection of personal data also poses the risk that the information could be used to extort intelligence officials or military servicemembers for political favors.[107] Hostile foreign actors could recover sensitive personal information about servicemembers' children, spouses, family and friends, using the data collection techniques discussed above. Such information could allow these actors to build detailed profiles on government officials, including their childrens' schools, spouse's workplaces, personal bank account information, etc. Those profiles could then be used to "plot all kinds of actual malevolence . . . . or to simply craft very precise threats toward their families" in order to retrieve confidential information or create paranoia.[108]

Ultimately, the marketplace for data has inherent risks that cannot be ameliorated through bans on individual applications or even back-end regulation on companies. The personal data industry is too interconnected and opaque for that. Even if a ban prevents one company from providing data to a foreign government, there is nothing stopping hostile actors from hacking into databases or buying that information on the open market. No matter what path it takes, Americans' personal data in the hands of a hostile foreign government poses a threat to our national security. The only way to ensure our personal data stays out of the wrong hands is to limit its collection in the first place.

III. A MISAPPLICATION OF THE IEEPA TO DATA PRIVACY

Given the breadth and severity of the personal data security risk, one might think that a new administration would have imposed a broad regulatory scheme to enhance data protection. However, the Trump Administration criticized comprehensive legislation, and instead adopted an ad hoc approach.[109] In banning TikTok as described above, President Trump did little to impact the broader problem, i.e., the opacity of the data marketplace and its inability to prevent personal

106. *See* Chen, *supra* note 104, at 8 (describing how the database allows intelligence officials to spot, assess, and develop potential recruits).

107. Dunlap, *supra* note 105 at 115.

108. *Id.*

109. *See* Mulligan, *supra* note 35, at 51–52 (describing how the Trump administration perceived "regulator-focused pirvacy policies and check boxes" as only serving "a very small number of users").

data from ending up in the wrong hands.

The use of the IEEPA, in particular, evinces a misunderstanding of the threat. Accordingly, this Part will examine the IEEPA in its application to cybersecurity issues stemming from TikTok. The use of the IEEPA to regulate data privacy is inappropriate (and, arguably, unlawful) for three reasons. First, the IEEPA was designed to combat unusual and extraordinary threats, not the ongoing and widespread data security crisis. Second, the TikTok ban violates the IEEPA exclusion on "informational materials." Finally, as a policy matter, Congress should have a greater role in regulating data security than an IEEPA framework would permit.

A. The IEEPA Was Not Intended to Apply to Widespread Threats

Using the IEEPA to combat ongoing threats contravenes its legislative purpose. Employing IEEPA powers should be narrowly tailored to respond to a "true" national emergency, an "unusual and extraordinary threat."[110] Instead, Presidents have invoked the statute broadly, and critics have recognized that the IEEPA is ripe for abuse.[111] As one commentator noted, "[t]hese uses suggest that the statute can and will be invoked whenever the President desires to draw on its broad powers, whether or not there is a genuine emergency."[112] Despite this overbroad usage, courts are reluctant to question a President's declaration of a national emergency.[113]

The first time the IEEPA was invoked was a true national emergency. During the Iran hostage crisis, two specific events constituted "unusual and extraordinary threat[s]" triggering President Carter's powers under the IEEPA: the taking of hostages by Iranian students with the endorsement of the insurgent party in Iran and the insurgent party's threat to withdraw Iranian funds from U.S.

110. *Trading With the Enemy Act Reform Legislaton: Hearing and Markup before the H. Comm. on Int'l Rel. on H.R. 7738*, 95th Cong. 14 (1977).

111. *See* Peter Harrell, *The Right Way to Reform the U.S. President's International Emergency Powers*, JUST SECURITY (Mar. 26, 2020), https://www.justsecurity.org/69388/the-right-way-to-reform-the-u-s-presidents-international-emergency-powers/ (noting that the IEEPA's broad grant of power to the president may allow a quick governmental response in times of genuine emergency, but that the statute's breadth renders it easily abused).

112. Jules Lobel, *Emergency Power and the Decline of Liberalism*, 98 YALE L. J. 1385, 1415 (1989) (quoting Carter, *International Economic Sanctions*, 75 CALIF. L. REV. 1159, 1235 (1987)).

113. *See* Koh, *supra* note 25, at 1313 (descrbing how the Court's "decisions on the merits of foreign affairs claims have enouraged a steady fllow of policymaking power from Congress to the Executive").

institutions.[114] As the House Report reviewing these events noted, "[s]uch a triggering of the IEEPA . . . was certainly consistent with the legislative history of that act."[115] In this case, the inciting incidents were isolated and identifiable.

Although use of the IEEPA should be limited to true national emergencies, oftentimes its application does not appear to meet the threshold for an unusual and extraordinary threat, as required under the statute. For example, multiple presidents have declared national emergencies in order to reinstate export regulations that were initially developed and passed by Congress.[116] In particular, President Reagan used the IEEPA to extend the Export Administration Act when Congress failed to renew the Act itself.[117] Commentators recognized that classifying the renewal as a "national emergency" stretched the standards for application of the IEEPA.[118] Regardless, a district court held that this did not contravene the statute because Congress had not amended he IEEPA to *prohibit* that practice.[119]

President Trump's ban on TikTok is far more similar to the latter application of the IEEPA. If the ban were enacted, President Trump would subvert the intent of the IEEPA. Declaring a national emergency under such circumstances would serve no other purpose but to further his own political agenda. Although ineffective personal data privacy regulation does pose a grave national security threat, TikTok itself is an insignificant fragment of that risk. TikTok alone cannot meet the threshold of an unusual and extraordinary threat as required by the IEEPA. Whereas the Carter Administration imposed appropriately long-term remedies to confront an unusual emergency threat,[120] the Trump Administration proposes a short-term solution to an endemic cybersecurity risk.

---

114. *See* STAFF OF H. COMM. ON BANKING, FIN. & URB. AFF., 97TH CONG., 1ST SESS., IRAN: THE FINANCIAL ASPECTS OF THE HOSTAGE SETTLEMENT AGREEMENT, 1213 (Comm. Print 1981) (noting that President Carter froze Iranian assets in response to the "barbaric political actions of the Iranian students" and the statement by an Iranian spokesman that Iran would repudiate all U.S. debts and withdraw its funds from U.S. depository institutions).

115. *Id.* at 12.

116. *See* CASEY ET AL., *supra* note 21, at 41–42 (noting that President Reagan was the first to use the IEEPA to extend export controls); *see also* Joel B. Harris & Jeffrey P. Bialos, *The Strange New World of United States Export Controls under the International Emergency Economic Powers Act*, 18 VAND. J. TRANSNAT'L L. 71, 81 (1985) (discussing President Reagan's use of the IEEPA).

117. *Id.* at 82.

118. *Id.*

119. United States v. Groos, 616 F. Supp. 2d 777, 785 (N.D. Ill. 2008).

120. These "long-term remedies" include economic sanctions that, to this day, shape the context of U.S.-Iran relations. *See* Casey et al., *supra* note 21, at 18–19.

Further, the use of the IEEPA to ban TikTok is questionable because it insulates the President's decision from judicial scrutiny and obscures the scale and scope of the dangers of data mining. First, the courts' tendency to refuse review of IEEPA actions makes challenging the ban particularly difficult. Given the broad discretion granted to the President under IEEPA precedent, a court might refuse to hear legitimate constitutional challenges on the grounds that invoking the IEEPA raises a nonjusticiable political question.[121] If that's the case, proponents of a comprehensive data privacy framework would have little opportunity to oppose this ad hoc approach, and would require Congress to pass alternative legislation undermining the executive order before comprehensive legislation could be implemented.

More importantly, regulating TikTok under the guise of a national emergency signals that TikTok is an isolated problem and obscures the scale of the threat. As explained in Part II, the transfer of Americans' personal data to hostile actors does pose a national security concern. However, TikTok's data mining practices do not pose an unusual and extraordinary threat to Americans. Rather, the information TikTok collects is typical of the industry writ large.[122] Therefore, focusing a ban on TikTok alone is ultimately a distraction from a broader national security solution: tightening the regulation of what personal data could be collected.[123] It is vital that Americans fully understand the scope of the cybersecurity threat so that comprehensive legislation can be enacted to combat it.

B. The TikTok Ban Violates the IEEPA Carve-out on Personal Communications and Informational Materials

The TikTok ban is improper under the IEEPA because IEEPA specifically exempts "informational materials" and "personal communications" from its reach. Known as the "Berman Amendment," the revision to the statute was meant to obviate First Amendment challenges to IEEPA use:

> The authority granted to the President by this section does not

121. *See infra* Part III(B) for a discussion of some possible challenges.

122. *See* Kevin Collier, *TikTok a Privacy Threat? Sure, But So Are Most of Your Smartphone Apps*, NBC NEWS (July 13, 2020), https://www.nbcnews.com/tech/security/tiktok-privacy-threat-sure-so-are-most-your-smartphone-apps-n1233625 (noting that it is "the norm" for phone apps to collect location data, usernames, phone numbers, device tupes, and more).

123. *See* Aaronson, *supra* note 71, at 1819 (observing that Canadian and German governments have instead focused on regulating "where and how" data is stored rather than banning individual apps).

> 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 . . . . or the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds.[124]

Although the examples of informational materials may seem out of date, the legislative history of the Berman Amendment shows that Congress had intended for these limitations to apply broadly. In a House Report describing the purpose of the Amendment, the drafters noted that

> [T]he principle that no prohibitions should exist on imports to the United States of ideas and information if their circulation is protected by the First Amendment. That principle applies with equal force to the exportation of ideas and information from this country to the rest of the world. Accordingly, these sections also exempt informational materials and publications from the export restrictions that may be imposed under these acts.[125]

In Congress's formulation, then, any information protected by constitutional speech is excepted from the President's authority under the IEEPA. Congress has also expanded the exceptions under the Amendment, noting that informational materials may include technologies and software.[126]

However, judicial deference to the President might limit the scope of this exception. A recent case interpreting the Amendment remarked, "[w]ith the Berman Amendment . . . . Congress sought to ensure the robust exchange of informational materials would not be unduly inhibited . . . ."[127] However, that same court upheld IEEPA regulation of software on the narrow grounds that only informational materials

---

124. 50 U.S.C. § 1702(b).

125. H.R. Rep. No. 100-40, Part . 3, at 113 (1987).

126. *See* 31 C.F.R § 560.418 (2009) (Iranian sanction regulations state that technology and software transmitted to Iran would violate that sanction "unless that technology or software meets the definition of information and informational materials in [the Berman Amendment] . . . .").

127. *See* United States v. Amirnazmi, 645 F.3d 564, 586 (3d Cir. 2011). In this case, the defendant developed a software which allowed users to plan and study chemical reactions. The software was then sold to the state-sponsored National Petrochemical Company of Iran. Because the software required tailoring to the end-user *after* sale, it was not "fully created and in existence" at the point of sale, and therefore could be regulated under the IEEPA.

"fully created and in existence" were subject to the exception.[128] Because the software at issue was customizable, it was not "fully created."[129] The court concluded that regulation of those materials is "not sacrosanct" as a result of the Amendment.[130] This holding indicates that, although the Amendment restricts the President's IEEPA authority to some extent, deference to the executive likely overrides certain applications of the exception.

The language and purpose of the Berman Amendment squarely encompasses things like TikTok. TikTok clearly involves the "exportation of ideas and information" from users in the United States to users abroad, and vice-versa. As stated above, TikTok users produce and share short-form videos on any topic—this is tantamount to the "film" exception enumerated in the statute. These videos are the products of users' constitutionally protected speech. Indeed, this was the very reason why a federal district court blocked the TikTok ban in late September 2020.[131]

Depending on how broadly a court interprets the exception, it is hard to imagine a ban on any app, not just TikTok, that would *not* violate the Amendment. Consider, for example, a ban on WhatsApp, an application that allows users to send text messages, video calls, images, etc.[132] Although WhatsApp was founded in the U.S., it has been vulnerable to hackers, as evidenced by a recent spyware attack.[133] Say, hypothetically, that the hack was coordinated by a foreign government. If President Trump had used his IEEPA powers to ban WhatsApp, the ban would probably be challenged on Berman Amendment grounds. WhatsApp, like many other apps, involves users exchanging ideas and information—precisely what the exception is meant to protect.

To take an even broader perspective, a court might consider *any* transfer of personal data to be protectable under the exception as an

128. *Id.*
129. *Id.* at 588.
130. *Id.* at 587.
131. TikTok Inc. v. Trump, No. 1:20-cv-02658, 2020 U.S. Dist. LEXIS 177250, at *16–17 (D.D.C. Sept. 27, 2020).
132. Chandra Steele, *What Is WhatsApp? An Explainer*, PCMAG (Feb. 20, 2014), https://www.pcmag.com/news/what-is-whatsapp-an-explainer.
133. *See* Zak Doffman, *WhatsApp Users Beware: This Stupidly Simple New Hack Puts You At Risk—Here's What You Do*, FORBES (Jan. 25, 2020), https://www.forbes.com/sites/zakdoffman/2020/01/25/whatsapp-users-beware-this-stupidly-simple-new-hack-puts-you-at-riskheres-what-you-do/?sh=62047a5b1d76 (describing a WhatsApp vulnerability that allowed hackers to gain access to accounts by relying on users' "susceptibility to social engineering").

expression of speech. Commentators and courts are divided over the question of whether personal data is speech.[134] Given the complexity of these arguments, this debate is outside of the context of this Note. Suffice it to say that if data is speech, the IEEPA cannot touch personal data, and thus cannot be used to protect it.

C. Congress's Role in Regulating Data Privacy Should Be Enhanced

As a policy matter, Congress should have a greater role in regulating data security than the IEEPA framework allows. Although the IEEPA was designed to *enhance* Congress's role in foreign affairs, it has had the opposite effect. Presidents have used the IEEPA to impose unitary executive action while Congress has been sidelined.

Virtually none of the congressional oversight mechanisms in the IEEPA is effective. The primary tool in the original version of the IEEPA was a legislative veto of the President's emergency declaration. That provision states: "[t]he authorities described in subsection (a)(1) may not continue to be exercised under this section if the national emergency is terminated by the Congress by concurrent resolution . . . . and if the Congress specifies in such concurrent resolution that such authorities may not continue to be exercised under this section."[135] However, as a result of *INS v. Chadha*, which held that the legislative veto violated constitutional separation of powers, Congress would likely need a two-thirds majority (a veto-proof supermajority) to "veto" an emergency declaration.[136] In this era of hyper-partisanship, it is highly unlikely that any vote could garner that much support.[137]

Congress itself is to blame for neglecting some of its supervisory duties in this area. Although the IEEPA stipulates that Congress meet every six months to discuss existing national emergencies, Congress has

134. *Compare* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014) (arguing that data is speech) *with* Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 U.C.L.A. L. R. 1149 (2005) (arguing that data is not speech); Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501 (2015).

135. 50 U.S.C. § 1706(b) (2018).

136. *See* 462 U.S. 919, 935 (1983) (holding that Congress cannot void the exercise of power by the executive branch through concurrent resolution, and can act only through bicameral passage followed by presentment of the law to the President).

137. *See* Elizabeth Goitein, *How Congress Is Pushing Back Against Trump's Unprecedented Use of Emergency Powers*, WASH. POST (Sept. 25, 2020), https://www.washingtonpost.com/politics/2020/09/25/how-congress-is-pushing-back-against-trumps-unprecedented-use-emergency-powers/ (noting that a veto-proof supermajority would today be "nearly impossible to achieve").

not once fulfilled this requirement.[138] Coupled with the courts' hesitation to question the President's emergency powers, the bloated statute gives essentially limitless power to the President.

This lack of oversight is of concern to Congress. Currently, there are two bipartisan bills pending in Congress that would reinstate the oversight the enacting Congress intended. One of these proposals would impose a 30-day period after a national emergency is declared wherein Congress must vote to extend the emergency if they want it to continue.[139] As the sponsor of that proposal, Senator Mike Lee (R-UT) notes, "[t]he problem is that emergency powers are vulnerable to abuse; they can act as a cheat-code that undermines of system of separation of powers and enables the president to bypass the difficult work of enacting legislation."[140]

In effect, the IEEPA allows the President unilateral control over federal data privacy policy, unless Congress acts to implement its own legislation. Under the IEEPA, President Trump could have banned all applications that pose some sort of data security threat with origins outside the U.S.[141] That would include not just apps made in China, but those made in Russia or any other OFAC-listed country.[142] Not only would that be a step too far, it's unlikely to effectively address widespread data security concerns.[143]

The security risks attendant to personal data protection are important enough that Congress deserves a seat at the table. The President should not unilaterally dictate policy, even if national security issues are traditionally the province of the executive branch. Although data privacy incidents implicate foreign affairs, the interdependencies of online networks go beyond the foreign versus domestic binary. The data protection problem is not raised by unique threat actors or foreign adversaries, it is a far-reaching issue that has direct, domestic effects.

138. Elizabeth Goitein, *The Alarming Scope of the President's Emergency Powers*, ATLANTIC (Jan./Feb. 2019), https://www.theatlantic.com/magazine/archive/2019/01/presidential-emergency-powers/576418/.

139. Assuring that Robust, Thorough, and Informed Congressional Leadership is Exercised Over National Emergencies (ARTICLE ONE) Act, S. 764, 116th Cong. § 202(a) (2019).

140. *Sen. Lee Introduces ARTICLE ONE Act to Reclaim Congressional Power*, MIKE LEE: U.S. SEN. FOR UTAH (Mar. 12, 2019), https://www.lee.senate.gov/public/index.cfm/2019/3/sen-lee-introduces-article-one-act-to-reclaim-congressional-power.

141. Although in theory the Berman Amendment should prevent the President from banning any application that trades in informational materials, the fact that President Trump attempted to ban TikTok indicates that interpretations of what may qualify under the exception can differ.

142. *See supra* note 76 and accompanying text.

143. *See supra* Part II(A)–(C).

Therefore, the traditional foreign policy principle delegating authority to the President simply does not apply here.[144] Because the IEEPA codifies that principle, its use is inappropriate when applied to personal data privacy.

Instead, Congress needs to intervene. Only Congress has the ability to adopt the broad legislative reforms required to protect American's personal data,[145] and only Congress can unify fragmented federal and state law to bring the U.S. in accord with its international peers.[146] The alternative, entrusting data protection to industry and the executive branch, will leave U.S. citizens' personal data and the nation as a whole vulnerable to attack.

IV. FEDERAL DATA PRIVACY REGULATION

Relying on the IEEPA to protect Americans' data privacy is an untenable solution. Although the government is not wrong to view the data privacy threat that TikTok and other similar services present as a national security risk, threats to data privacy are ubiquitous and cannot be dealt with through unitary executive action under the IEEPA. A comprehensive problem requires a comprehensive solution.

Reviewing the deficiencies of the IEEPA raises the question: Is there a way to regulate personal data that (1) sufficiently tackles the breadth of the cybersecurity issue, (2) avoids First Amendment free speech challenges, and (3) incorporates both congressional and executive branch concerns? Any effective legislation would also need to address the problem at its source—i.e. what data can be collected and what companies can do with that data.

California's Consumer Privacy Act (CCPA) provides a model for such national legislation.[147] Although the CCPA is costly and raises

144. Much has been written about separation of powers in the realm of foreign affairs. Judicial interpretations have generally upheld the President's broad discretion in this area. *See, e.g.*, United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936) (holding that "the President [is] is the sole organ of the federal government in the field of international relations"); *but see* Youngstown Sheet and Tube Co. v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring) (stating that "[w]hen the President acts in absence of either a congressional grant or denial of authority, he can only rely upon his own independent powers, but there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain").

145. U.S. CONST. art. I, § 8.

146. *See* Mulligan, *supra* note 35, at 3 ("This fragmented legal landscape coupled with concerns that existing federal laws are inadequate has led many stakeholders to argue that the federal government should assume a larger role in data protection policy.").

147. Cal. Civ. Code § 1798.100 (West 2020).

potential federalism issues, it exemplifies a much-needed effort to proactively regulate data privacy. The CCPA protects consumer privacy at the point of collection, regulates what companies may do with personal data, and avoids the defects of an ad hoc method. Although the CCPA is not a complete solution, it provides a framework for workable federal legislation.

A. The CCPA

The CCPA began as a 2017 ballot initiative for sweeping changes to existing privacy law. The purpose of the bill was to protect individuals' "inalienable" right to privacy, fundamental to which was the "ability of individuals to control the use, including the sale, of their personal information."[148]

The legislation, which took effect in early 2020, provides that any business operating in California that meets certain criteria must comply with several regulations relating to personal data security.[149] First, businesses that sell personal data (including data brokers) must give consumers the right to opt out of the sale if they request.[150] Second, consumers can request that businesses disclose whatever personal information they have collected, why they collected it, and what was done with the information.[151] Consumers are also afforded a private right of action in the event of a data breach.[152] Finally, consumers can request that businesses delete their personal data, and businesses must respond within 45 days.[153] Although not directly part of the CCPA, California law also requires that data brokers register with the state, another effort to increase transparency.[154] In providing consumers the tools to manage their data, the CCPA takes the initial step in reducing the ways that businesses can use that data. In doing so, the CCPA aims to protect consumer privacy at its source: the collection stage.

On a federal level, the enactment of the CCPA drew renewed

148. A.B. 375, 2019 Cal. St. Assemb. (Cal. 2019).

149. *See* Cal. Civ. Code § 1798.105 –140(c) (West 2020) ("The CCPA applies to for-profit businesses that do business in California and meet any of the following: have a gross annual revenue of over $25 million; buy, receive, or sell the personal information of 50,000 or more California residents, households, or devices; or derive 50% or more of their annual revenue from selling California residents' personal information.").

150. *Id.* at § 1798.05(a).

151. *Id.* at § 1798.110(a).

152. *Id.* at § 1798.150(a).

153. *Id.* at §1798.130(a)(2)(A).

154. *Id.* at §§ 1798.99.80–88.

attention to data privacy.[155] Several bipartisan legislative proposals modeled on the CCPA have been introduced.[156] Despite broad agreement on the need to create a federal data protection law, these recently introduced and past legislative proposals have been held up in Congress.[157] To appreciate why requires an understanding of the policy debate at the heart of these issues: the primacy of data privacy versus the economic and political risks in enacting those policies.

First, lobbyists decried the CCPA's financial costs.[158] Initial CCPA compliance for companies in California was projected to cost up to $55 billion.[159] The costs of implementation and compliance on a national level would, of course, be drastically higher. And beyond the immediate financial costs are potential future costs to the advertising industry. By limiting access to personal data, targeted advertising may be similarly curtailed.[160] Limiting behavioral advertising may also have significant downstream effects on the economy.[161] Although those financial consequences deserve due consideration, they simply cannot outweigh the necessity of comprehensive data privacy legislation. Though the financial costs of compliance would be significant, the impacts of not complying transcend purely economic concerns. Without personal data privacy protection, we risk a repeat of the Cambridge Analytica incident, of further data breaches, and of greater threats to our national security.[162]

Second, consumer privacy advocates protested that the CCPA did

155. *See* David McCabe, *Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight.*, N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html ("[Tech] industry groups flooded Washington with a clear message meant to neutralize California's rules entirely. Congress should pass a national privacy law, they said, and include a provision superseding any state legislation on the issue.").

156. *See generally* Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act, S. 3663, 116th Cong. (2020); *see also* Data Broker Accountability and Transparency Act of 2020, H.R. 6675, 116th Cong. (2020).

157. *See* McCabe, *supra* note 151 and accompanying text.

158. *Id.*

159. Caitlin Chin, *Highlights: The GDPR and CCPA as Benchmarks For Federal Privacy Legislation*, BROOKINGS INST. (Dec. 19, 2019), https://www.brookings.edu/blog/techtank/2019/12/19/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/.

160. *See* Theodore F. Claypoole, *Will CCPA Kill Advertising as We Know It?*, 10 NAT'L L. REV. 1, 2 (2020) (noting that the regulation could allow consumers to avoid targeted advertising through browser plug-ins.).

161. *See id.*("Data is the currency of this advertising world, and the CCPA if strictly enforced could cripple many of the advances made in the past 30 years.").

162. *See supra* Part II(C) for a discussion of how national security concerns include the spread of propaganda and targeting of intelligence and military officials.

not go far enough in protecting personal data.[163] These activists asserted that the CCPA would not adequately protect consumer data because it shifts much of the burden onto consumers to affirmatively exercise their rights.[164] In that sense, the CCPA does not constrain data collection at all.[165] However, this argument misses the point of the CCPA. The legislation was always meant to act as an initial step towards privacy protection, rather than as a sweeping defense of consumer rights.[166] And still, the CCPA is widely considered the most extensive data protection regime in the United States.[167] In fact, the CCPA's status as a baseline measure has already been proven. In November 2020, California voters approved the California Privacy Rights Act (CPRA), which expands the CCPA's opt-out right and private right of action, and institutes a privacy regulatory body and a right to correct personal information under the CCPA.[168]

Finally, those concerned that the CCPA might provide a basis for federal legislation wondered how a "federal CCPA" might preempt existing state privacy law. Several states have enacted legislation similar to the CCPA,[169] but may differ in some important respects.[170] Here, a federal CCPA could provide a floor, rather than a ceiling, for state law. In other words, federal legislation would preempt existing state law, but only to the extent that state law fails to meet the standards outlined by the CCPA.[171]

---

163. *See e.g.*, GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation: Hearing Before the S. Comm. on the Judiciary, 116th Cong. 1 (2019) (Statement of Michelle Richardson, Director, Privacy & Data Center for Democracy & Tech.) ("Privacy self-management alone is neither scalable nor practical for the individual. Burdening individuals with more and more granular decisions, absent some reasonable boundaries, will not provide the systemic changes we need.").

164. *Id.*

165. *Id.*

166. *See* Revisiting the Need for Data Privacy Legislation: Hearing Before the S. Comm on Com., Sci. and Transp., 116th Cong. 2 (2020) (Statement of Xavier Becerra, Attorney General of the State of California) ("Like any law, the CCPA is not perfect, but it is an excellent first step.").

167. *Id.*

168. *See* The California Privacy Rights Act of 2020, CA Proposition 24 (2020).

169. Currently, only Virginia and Nevada have passed legislation similar to the CCPA, but legislation is pending in 24 other states. *See* Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, IAPP WESTIN RESEARCH CTR., https://iapp.org/resources/article/state-comparison-table/ (last visited Mar. 6, 2021).

170. *See* Mulligan, *supra* note 35, at 37 (noting that the CCPA is particularly comprehensive relative to many other states' laws).

171. Arguably, this preemption approach would fail to unify state and federal law, as no single national data privacy standard would exist. *See* Cameron F. Kerry and John B. Morris, Jr., *Preemption: A Balanced National Approach to Protecting all Americans' Privacy*, LAWFARE (June 18, 2020), https://www.lawfareblog.com/preemption-balanced-national-approach-protecting-all-americans-privacy.

B. The CCPA Overcomes the Deficiencies of an Ad Hoc Method

Implementing legislation similar to the CCPA would also help address the three deficiencies of the IEEPA method: that ad hoc solutions do not comprehensively protect consumer privacy, any outright ban would encounter First Amendment challenges, and it permits unitary executive action when the decisionmaking process should include Congress.

First, applying the CCPA on a federal level would represent an initial effort at combating the dangers of the data marketplace: namely, system hacks, data sharing with foreign governments, and selling personal data to hostile actors.[172] To limit the likelihood of a hack, the CCPA gives consumers a private right of action in the event of a data breach. On a national level, this would encourage businesses to implement data protection measures on their own, such as limiting the amount of personal data collected, and deleting that data automatically when it is no longer needed. Also, the CCPA reduces the risk of data ending up in the hands of hostile actors because the Act gives consumers the right to limit the data they provide and sell. In short, the CCPA gives consumers dominion over their data.

Furthermore, a national CCPA would not implicate First Amendment issues. Under the CCPA, consumers are free to create and share whatever information they want—they just have more control over where it ends up. Further, courts have recognized that a certain amount of privacy aids free expression and free association.[173] In that sense, encouraging basic data protection could safeguard against these concerns.

Finally, implementing the CCPA would require the cooperation of Congress. Given the patchwork of data privacy laws across the country, it is particularly important that a federal law harmonizes these approaches, understanding both industry and consumer considerations. Only Congress is suited to do that. As state data privacy laws gain momementum and bipartisan support for a federal approach builds, the time is ripe for Congress to enact meaningful legislation.

Although a federal version of the CCPA would not eliminate all of

172. *See supra* Part II(A)-(C).

173. *See, e.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (holding that "[a]nonymity is a shield from the tyranny of the majority . . . . It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society").

the concerns presented by the mining of personal data, it is a solid foundation to initially address personal data privacy issues. Legislators must keep in mind that as time passes, the more personal data is collected and the more these risks are exacerbated. Therefore, Congress must act swiftly. Implementing legislation based on the existing CCPA framework represents the most efficient route to begin protecting Americans' personal data.

CONCLUSION

The use of the IEEPA to ban TikTok, an ad hoc solution directed by the President, represents a flawed approach for the future of our national data privacy policy: the approach has been shown to be legally untenable and does not provide a comprehensive solution. Banning individual apps is insufficient to tackle the opacity of the personal data marketplace, the amount of data that is collected, and the many ways that data may be compromised. Inadequate data protection will continue to pose the risk that individual Americans' personal data ends up in the wrong hands. An ambitious effort to develop comprehensive data privacy protection must be enacted, based on the foundation provided by the CCPA. The longer Congress waits to implement this legislation, the more the nation risks exposure to further unforeseen privacy attacks.