Oklahoma Law Review

Volume 74 | Number 3

2022

TikTok, WeChat, and National Security: Toward a U.S. Data Privacy Framework

Robert L. Rembert

TikTok, WeChat, and National Security: Toward a U.S. Data Privacy Framework

Table of Contents

Introduction

> *The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.*[1]

On August 6, 2020, President Donald J. Trump issued two Executive orders (the "Executive Orders," or the "Orders") targeting Chinese technology companies TikTok and WeChat.[2] TikTok, a video-sharing

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

2. Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020) [hereinafter TikTok Order] (ordering sale of TikTok); Exec. Order No. 13,943, 85 Fed. Reg. 48,641 (Aug. 6, 2020) [hereinafter WeChat Order] (blocking transactions with WeChat).

mobile application, had seen a precipitous rise in popularity, primarily among teenagers;[3] before the August 2020 Orders, TikTok had been downloaded 175 million times in the United States[4] and had 50 million active users.[5] WeChat, considered the "digital bedrock of daily life" in China,[6] is China's largest messaging platform;[7] 1.2 billion people use it every month,[8] and there are an estimated 19 million users in the United States alone.[9]

The Orders prohibited transactions between persons subject to U.S. jurisdiction and the two Chinese technology companies,[10] which rendered the applications "essentially useless within the United States."[11] For WeChat, this prevented U.S. users from using WeChat to send money to family members, friends, and businesses in China.[12] WeChat users in the United States were also unable to download or update the app, which prevented security updates and threatened to degrade the app's utility over time.[13] The TikTok Order gave TikTok's parent company, ByteDance, forty-five days to sell its subsidiary to a U.S. company, and if it failed to

3. Raymond Zhong & Sheera Frenkel, *A Third of TikTok's U.S. Users May Be 14 or Under, Raising Safety Questions*, N.Y. TIMES (Sept. 17, 2020), https://www.nytimes.com/2020/08/14/technology/tiktok-underage-users-ftc.html.

4. TikTok Order, *supra* note 2.

5. Brian X. Chen, *What Is Happening with TikTok and WeChat as Trump Tries to Ban Them?*, N.Y. TIMES (Sept. 18, 2020), https://www.nytimes.com/2020/09/18/technology/tiktok-wechat-ban.html.

6. Paul Mozur & Raymond Zhong, *Targeting WeChat, Trump Takes Aim at China's Bridge to the World*, N.Y. TIMES (Sept. 4, 2020), https://www.nytimes.com/2020/08/07/business/trump-china-wechat-tiktok.html?action=click&module=RelatedLinks&pgtype=Article.

7. 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/.

8. Mozur & Zhong, *supra* note 6.

9. Kokas, *supra* note 7.

10. TikTok Order, *supra* note 2; WeChat Order, *supra* note 2.

11. Ana Swanson et al., *Trump Administration to Ban TikTok and WeChat from U.S. App Stores*, N.Y. TIMES (Sept. 18, 2020), https://www.nytimes.com/2020/09/18/business/trump-tik-tok-wechat-ban.html.

12. Shelly Banjo et al., *Trump Backs Threats Against China with TikTok, WeChat Bans*, BLOOMBERG (Sept. 18, 2020, 10:37 PM CDT), https://www.bloomberg.com/news/articles/2020-09-18/u-s-to-block-some-wechat-tiktok-transactions-as-of-sunday.

13. *Id.*

reach a deal within forty-five days, the United States would ban the app entirely.[14]

The Orders invoked national security as a rationale for blocking transactions with TikTok and WeChat. Under Chinese law, the Chinese government may compel companies in China to turn over users' personal data, and there has been growing U.S. concern that subsidiaries of Chinese companies operating in the United States can transfer U.S. citizens' personal data to parent companies subject to data requests from the Chinese government.[15] These concerns are warranted—TikTok's privacy policy states that the company "may share all of the information [it] collect[s] with a parent, subsidiary, or other affiliate of [its] corporate group."[16] As the Orders highlighted, the national security concern is that these companies' collection of "vast swaths" of personal information "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information."[17] The Orders further explained that access to this data would enable the Chinse government to track federal employees' physical movements, build dossiers of personal information to blackmail U.S. citizens, and "conduct corporate espionage."[18]

President Trump issued the Orders targeting TikTok and WeChat[19] under the authority granted by the International Emergency Economic Powers Act ("IEEPA").[20] IEEPA grants the President broad authority to regulate commerce after declaring a "national emergency" to address "any unusual and extraordinary threat . . . to the national security, foreign policy, or economy of the United States."[21] In this case, the President used IEEPA to block transactions with the two Chinese technology companies; this was the first time a President had invoked international emergency powers to

14. Rachel Lerman, *'45 Days of Ambiguity': What a U.S. TikTok Ban Could Mean for Users and Employees*, WASH. POST (Aug. 17, 2020), https://www.washingtonpost.com/technology/2020/08/17/tiktok-ban-us-faq/.

15. Alex Schiller, *WeChat and TikTok: Paper Tigers or Threats to U.S. National Security?*, CHINA FOCUS (Sept. 28, 2020), https://chinafocus.ucsd.edu/2020/09/28/wechat-and-tiktok-paper-tigers-or-threats-to-u-s-national-security/.

16. *Legal: Privacy Policy*, TIKTOK, https://www.tiktok.com/legal/privacy-policy?lang=en (June 2, 2021).

17. TikTok Order, *supra* note 2; WeChat Order, *supra* note 2.

18. TikTok Order, *supra* note 2; *see also* WeChat Order, *supra* note 2 (asserting that the spread of mobile applications from Chinese companies "continues to threaten the national security, foreign policy, and economy of the United States").

19. TikTok Order, *supra* note 2; WeChat Order, *supra* note 2.

20. 50 U.S.C. §§ 1701–1707.

21. *Id.* § 1701.

address threats posed by popular consumer applications.[22] But a federal court enjoined the WeChat Order on First Amendment grounds,[23] and another federal court enjoined the TikTok Order based on an IEEPA provision prohibiting the direct or indirect regulation of "personal communication[s]" and the exchange of "informational materials."[24] In June 2021, President Biden revoked the Orders entirely.[25]

The Executive Orders targeting TikTok and WeChat have highlighted that IEEPA is too narrow a tool to address the national security challenges that foreign technology companies pose to U.S. interests. And even if the Orders had successfully blocked the Chinese government's ability to access U.S. citizens' personal data through TikTok and WeChat, the Orders still would not have meaningfully reduced the threat. First, TikTok and WeChat are only two companies out of a multitude of foreign companies operating in the United States.[26] Other foreign-owned mobile applications have also received scrutiny for their data collection practices and for threatening national security, such as FaceApp, the age-enhancing selfie app that went viral in 2019.[27] Data harvesting is so pervasive[28] that even if the Orders were completely effective in protecting user data collected by TikTok and WeChat, they would fail to address the more fundamental issues of data security and privacy. In fact, the Orders were more likely to distract from

22. Lerman, *supra* note 14.

23. U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912, 930 (N.D. Cal. 2020).

24. TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 102, 115 (D.D.C. 2020) (alteration in original).

25. Jeanne Whalen & Ellen Nakashima, *Biden Revokes Trump's TikTok and WeChat Bans, but Sets Up a Security Review of Foreign-Owned Apps*, WASH. POST (June 9, 2021, 1:33 PM EST), https://www.washingtonpost.com/technology/2021/06/09/tiktok-ban-revoked-biden/.

26. *See* Kristen Bialik, *Number of U.S. Workers Employed by Foreign-Owned Companies Is on the Rise*, PEW RSCH. CTR. (Dec. 14, 2017), https://www.pewresearch.org/fact-tank/2017/12/14/number-of-u-s-workers-employed-by-foreign-owned-companies-is-on-the-rise/; Mary Hanbury, *11 American Companies That Are No Longer American*, BUS. INSIDER (Aug. 2, 2018, 2:03 PM), https://www.businessinsider.com/american-companies-that-are-no-longer-american-2017-6.

27. Thomas Brewster, *FaceApp: Is the Russian Face-Aging App a Danger to Your Privacy?*, FORBES (July 17, 2019, 7:20 AM EDT), https://www.forbes.com/sites/thomasbrewster/2019/07/17/faceapp-is-the-russian-face-aging-app-a-danger-to-your-privacy/#64aacfdc2755.

28. Madeline M. Cook, Comment, *Bringing Down Big Data: A Call for Federal Data Privacy Legislation*, 74 OKLA. L. REV. (forthcoming 2022).

these issues and give a false sense of security to mobile app users. As one scholar has said, the Orders were "merely window dressing."[29]

Second, American companies also collect the "vast swaths"[30] of data that the Orders describe will fall into the hands of foreign governments.[31] From browser extensions that collect information about every website you visit[32] to applications that harvest and sell your location data,[33] American companies arguably know you better than you know yourself.[34] And foreign actors can still gain that information from American companies. For example, a hack of the company Equifax in 2017 which the Department of Justice attributed to four members of China's military exposed the personal data of up to 147.9 million U.S. consumers.[35]

Invoking IEEPA to block foreign technology companies' access to U.S. user data on a case-by-case basis is wholly inadequate. Instead, the United States should adopt a federal data privacy law that could more effectively protect national security interests and safeguard data privacy. Part I of this Comment examines the development of IEEPA and argues that it is an inadequate tool for protecting national security and data privacy from private sector applications that collect unprecedented amounts of personal information. Part II then examines federal data privacy legislation as a superior alternative to IEEPA for protecting national security and safeguarding U.S. citizens' personal information. This Part further looks to the European Data Protection Regulation ("GDPR") and various

29. Kokas, *supra* note 7.

30. WeChat Order, *supra* note 2; Tiktok Order, *supra* note 2.

31. *See* Greg Bensinger, *Trump Wants to Cripple TikTok and WeChat. Why?*, N.Y. TIMES (Sept. 18, 2020), https://www.nytimes.com/2020/09/18/opinion/wechat-tiktok-trump.html ("There's irony in the United States taking exception to TikTok and WeChat's data collection when our homegrown technology giants have built their empires on hoovering up more and more of our personal information.").

32. Geoffrey A. Fowler, *I Found Your Data. It's for Sale*, WASH. POST (July 18, 2019), https://www.washingtonpost.com/technology/2019/07/18/i-found-your-data-its-sale/.

33. Zack Whittaker, *Data Brokers Track Everywhere You Go, but Their Days May Be Numbered*, TECHCRUNCH (July 9, 2020, 8:00 AM CDT), https://techcrunch.com/2020/07/09/data-brokers-tracking/.

34. *See, e.g.*, James Carmichael, *Google Knows You Better Than You Know Yourself*, ATLANTIC (Aug. 19, 2014), https://www.theatlantic.com/technology/archive/2014/08/google-knows-you-better-than-you-know-yourself/378608/.

35. Yashaswini Swamynathan, *Equifax Reveals Hack That Likely Exposed Data of 143 Million Customers*, REUTERS (Sept. 7, 2017, 3:49 PM), https://www.reuters.com/article/us-equifax-cyber/equifax-says-hack-potentially-exposed-details-of-143-million-consumers-idUSKCN1BI2VK; Brian Barrett, *How 4 Chinese Hackers Allegedly Took Down Equifax*, WIRED (Feb. 10, 2020, 12:52 PM), https://www.wired.com/story/equifax-hack-china/.

approaches to data privacy that have been proposed in the United States. Part II concludes that a federal data privacy law should incorporate the GDPR's regulation of cross-border data flows, which would both ameliorate the risks that foreign technology companies pose to U.S. national security interests and prevent other companies from compromising U.S. citizens' privacy interests as TikTok and WeChat have.

Ultimately, the TikTok and WeChat situation has demonstrated the weakness of the United States' data privacy framework and the pressing need for lawmakers to enact legislation that will both protect national security and safeguard the right to privacy. This Comment shows that federal data privacy legislation, while not the panacea for national security and data privacy challenges, would be a step in the right direction. Perhaps the silver lining of the TikTok and WeChat debacle is that it will help shift the United States toward a more comprehensive data privacy framework.

I. The International Emergency Economic Powers Act

This Part assesses the adequacy of IEEPA as a tool to address the national security issues that arise when a foreign government has the power to acquire U.S. citizens' personal data. Section I.A provides an overview of IEEPA's purpose and historical practice, demonstrating that Presidents have invoked IEEPA in an increasingly broad array of situations.[36] Section I.B then provides background on TikTok and WeChat and analyzes how the Executive Orders illustrate IEEPA's shortcomings in addressing threats that foreign mobile applications pose to U.S. national security. This Part concludes that (1) IEEPA is an unsuitable response to national security issues posed by TikTok, WeChat, and other mobile applications that harvest user data and that (2) federal data privacy legislation would better protect national security.

A. History

In 1977, Congress enacted IEEPA as a response to the increasingly broad use of another presidential emergency power: the Trading with the Enemy

36. While this broadened use has caused scholars to argue for amendments to IEEPA, this is beyond this Comment's scope. For a discussion of IEEPA reform, see Andrew Boyle, *Trump's Latest Abuse of Emergency Powers Highlights a Dangerous Law in Need of Change*, BRENNAN CTR. FOR JUST. (June 24, 2020), https://www.brennancenter.org/our-work/analysis-opinion/trumps-latest-abuse-emergency-powers-highlights-dangerous-law-need-change, and Jason Luong, Note, *Forcing Constraint: The Case for Amending the International Emergency Economic Powers Act*, 78 TEX. L. REV. 1181 (2000).

Act of 1917 ("TWEA").[37] After the United States entered into World War I, Congress enacted TWEA to grant the President broad authority to regulate international transactions with foreign enemies.[38] TWEA section 5(b) contained the heart of this authority, which "gave the President expansive control over private international economic transactions."[39] While TWEA's original text only granted the President authority to regulate international transactions in times of war, Congress amended section 5(b) in 1933 to allow the President to regulate transactions in peacetime.[40] As amended, the statute provided the following:

> During time of war *or during any other period of national emergency declared by the President*, the President may, through any agency that he may designate, or otherwise, investigate, regulate, or prohibit, under such rules and regulations as he may prescribe, by means of licenses or otherwise, any transactions in foreign exchange, transfers of credit between or payments by banking institutions as defined by the President . . . .[41]

By the Cold War, TWEA had become a popular economic sanctions tool in foreign policy.[42] In the 1970s, however, Congress sought to curtail what it viewed as "extensive use by Presidents of emergency authority . . . to regulate both domestic and international economic transactions unrelated to a declared state of emergency."[43]

IEEPA was a response to this extensive use.[44] Congress intended to limit the President's powers during peacetime, which had become "essentially an unlimited grant of authority [under TWEA]," to be limited to times of national emergency.[45] Congress thus modified TWEA section 5(b) to allow for the regulation of international transactions only in times of war and authorized the President to regulate international transactions in peacetime

37. Note, *The International Emergency Economic Powers Act: A Congressional Attempt to Control Presidential Emergency Power*, 96 HARV. L. REV. 1102, 1102 (1983).

38. CHRISTOPHER A. CASEY ET AL., CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE 3–4 (2020), https://crsreports.congress.gov/product/pdf/R/R45618.

39. *Id.*

40. *Id.* at 5.

41. H.R. 1491, 73d Cong. (1933) (emphasis added) (enacted).

42. CASEY ET AL., *supra* note 38, at, at 6.

43. S. REP. NO. 95-466, at 2 (1977).

44. *Id.* at 2, 4.

45. H.R. REP. NO. 95-459, at 7 (1977).

under IEEPA.[46] But to regulate transactions under IEEPA, the President must first declare a national emergency under the National Emergencies Act of 1976 ("NEA").[47] A national emergency was to be "rare and brief" and should not "be equated with normal, ongoing problems."[48] Congress further emphasized that IEEPA "should be available only in true emergencies."[49] And while Congress did not define a "true emergency," IEEPA's text provides that any emergency must relate to an "unusual or 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."[50]

NEA also provided procedural safeguards for declaring a national emergency.[51] These safeguards required the President to consult with Congress before declaring a national emergency, terminated the national emergency after one year unless the President renewed it, and empowered Congress to override the President's declaration of a national emergency through a concurrent resolution.[52]

Furthermore, IEEPA provided for several exceptions to the President's authority to regulate transactions, including a prohibition on directly or indirectly regulating the following:

- "personal communication[s]" that do not "involve a transfer of anything of value";[53]
- donations "intended to be used to relieve human suffering";[54] or
- the importation of "information or informational materials, including but not limited to, publications, films, posters,

46. L. ELAINE HALCHIN, CONG. RSCH. SERV., 98-505, NATIONAL EMERGENCY POWERS 10 (2021), https://fas.org/sgp/crs/natsec/98-505.pdf.

47. *See* H.R. REP. NO. 95-459, at 6.

48. *Id.* at 10.

49. *Id.* at 12.

50. 50 U.S.C. § 1701.

51. HALCHIN, *supra* note 46, at 11.

52. *Id.* After the Supreme Court's decision in *Immigration & Naturalization Service v. Chadha*, 462 U.S. 919 (1983), which invalidated concurrent resolutions, Congress amended the NEA to require a joint resolution to override a national emergency. HALCHIN, *supra* note 46, at 11. This had the effect of making any override of a national emergency declaration extremely unlikely since the President would need to sign off on the joint resolution.

53. 50 U.S.C. § 1702(b)(1).

54. *Id.* § 1702(b)(2).

> phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds."[55]

Overall, Congress intended IEEPA to strike a balance between "executive flexibility" in addressing foreign threats with "political accountability."[56]

Although Congress enacted IEEPA to reign in executive declarations of national emergencies, Presidents have invoked IEEPA in an increasingly broad array of situations, and the declared national emergencies have been anything but "rare and brief."[57] Presidents have invoked IEEPA fifty-nine times since 1977, and the average length of a national emergency is more than nine years.[58] The first national emergency was declared in 1979 in relation to the Iranian hostage crisis, and that national emergency is still in effect.[59] At the same time, IEEPA's emergency renewals have become a "pro-forma exercise,"[60] and a declaration of national emergency needs only contain "the magic words."[61] And while IEEPA was initially limited by specific geographical targets, it has expanded to address threats that transcend geography, such as global terrorism, cyberattacks, and drug trafficking.[62]

There is of course a benefit to allowing a President broad discretion in responding to a national security threat.[63] The President must be capable of declaring a national emergency (if one exists) and taking necessary measures to eliminate it. But the increasingly routine and expansive uses of IEEPA risk making IEEPA itself a barrier to achieving a more sustainable and comprehensive response to national security threats.

---

55. *Id.* § 1702(b)(3).

56. Note, *supra* note 37, at 1104.

57. CASEY ET AL., *supra* note 38, at 17.

58. *Id.*

59. *Id.* at 18–19.

60. Peter Harrell, *The Right Way to Reform the U.S. President's International Emergency Powers*, JUST SEC. (Mar. 26, 2020), https://www.justsecurity.org/69388/the-right-way-to-reform-the-u-s-presidents-international-emergency-powers/ (discussing proposals for procedural reform to IEEPA in light of its expanded use).

61. *What a President Can Do Under the International Emergency Economic Powers Act*, NPR: ALL THINGS CONSIDERED (May 31, 2019, 6:11 PM ET), https://www.npr.org/2019/05/31/728754901/what-a-president-can-do-under-the-international-emergency-economic-powers-act.

62. *Id.*; CASEY ET AL., *supra* note 38, at 17.

63. See generally Note, *supra* note 37, for a discussion of the benefits of broad executive authority under IEEPA.

B. The 2020 Executive Orders Targeting TikTok and WeChat

In one respect, the TikTok and WeChat Orders are not unique; they reflect the expanding use of IEEPA to address various threats to national security. They are different, however, in that they represent the first uses of IEEPA to target popular mobile phone applications.[64] Ultimately, both Orders faced constitutional challenges and federal courts enjoined their enforcement.[65] This Section first demonstrates that the threat to national security far exceeds TikTok and WeChat. This Section then examines how the legal challenges to the TikTok and WeChat Orders illustrate why IEEPA is incapable of addressing the threats that mobile applications pose to national security.

1. TikTok and WeChat

With more than 180 million downloads in the United States, TikTok's sudden rise in popularity perhaps represents the first time a foreign-developed mobile application has garnered such a devoted user base.[66] But it will not be the last.[67]

U.S. national security concerns stemmed from TikTok's corporate ownership structure, which made U.S. user data susceptible to access by the Chinese government. TikTok's parent company, ByteDance, is a Chinese tech company.[68] In 2016, ByteDance launched the China-based video application Douyin, and within a year, Douyin had 100 million users and one billion daily video views.[69] The following year, ByteDance began to

64. *See* Elizabeth Goitein, *How Congress Is Pushing Back Against Trump's Unprecedented Use of Emergency Powers*, WASH. POST (Sept. 25, 2020, 6:00 AM EDT), https://www.washingtonpost.com/politics/2020/09/25/how-congress-is-pushing-back-against-trumps-unprecedented-use-emergency-powers/.

65. TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 100, 115 (D.D.C. 2020); U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912, 916, 930 (N.D. Cal. 2020).

66. *See* Katy Stech Ferek & Liza Lin, *TikTok Files Suit Challenging U.S. Ban*, WALL ST. J. (Aug. 24, 2020, 3:24 PM ET), https://www.wsj.com/articles/tiktok-to-file-suit-challenging-u-s-ban-11598281193.

67. David E. Sanger, *TikTok Deal Exposes a Security Gap, and a Missing China Strategy*, N.Y. TIMES (Sept. 20, 2020), https://www.nytimes.com/2020/09/20/us/politics/tiktok-trump-national-security.html ("The longer-run issue, however, is that there will be more TikToks, companies around the world that develop apps that Americans love—or see as a hedge against their own government.").

68. Paige Leskin, *Inside the Rise of TikTok, the Viral Video-Sharing App Wildly Popular with Teens and Loathed by the Trump Administration*, BUS. INSIDER (Aug. 7, 2020, 4:20 PM), https://www.businessinsider.com/tiktok-app-online-website-video-sharing-2019-7.

69. *Id.*

expand Douyin internationally under the name TikTok.[70] Meanwhile, in the United States, the short-form video application Musical.ly was gaining popularity among teenagers.[71] In November 2017, ByteDance purchased Musical.ly, and in 2018, ByteDance merged Musical.ly with TikTok.[72] National security concerns led to an investigation of the merger by the Department of the Treasury's Committee on Foreign Investment in the United States,[73] which reviews transactions involving foreign investment in the United States to determine whether they present a national security risk.[74] Following the Committee's investigation, TikTok took numerous steps to assuage national security concerns, such as appointing an ex-Disney executive as its chief executive officer, launching a content advisory council to lead its policy changes, and establishing a transparency center to evaluate its data privacy and security practices.[75] But in the eyes of lawmakers and the President, these steps were inadequate to cure the national security threat posed by TikTok's connection to China.[76]

Most of the U.S. government's concerns relate to TikTok's ownership by ByteDance because it is subject to China's far-reaching cybersecurity law.[77] Under China's cybersecurity law, Chinese companies have broad obligations to assist the government in investigating political and ideological threats to the country.[78] While TikTok has publicly stated that it would refuse to cooperate with a request from the Chinese government to hand over U.S. users' personal data,[79] TikTok's privacy policy reveals that

---

70. *Id.*

71. *Id.*

72. *Id.*

73. *The Committee on Foreign Investment in the United States (CFIUS)*, U.S. DEP'T TREAS., https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius (last visited Feb 13, 2021).

74. Greg Roumeliotis et al., *Exclusive: U.S. Opens National Security Investigation into TikTok - Sources*, REUTERS (Nov. 1, 2019, 10:21 AM), https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-u-s-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL.

75. Leskin, *supra* note 68.

76. *Id.*

77. Jacob Helberg, *Silicon Valley Can't Be Neutral in the U.S.-China Cold War*, FOREIGN POL'Y (June 22, 2020, 5:18 PM), https://foreignpolicy.com/2020/06/22/zoom-china-us-cold-war-unsafe/.

78. *Id.*

79. Robert McMillan et al., *TikTok User Data: What Does the App Collect and Why Are U.S. Authorities Concerned?*, WALL ST. J. (July 7, 2020), https://www.wsj.com/articles/tiktok-user-data-what-does-the-app-collect-and-why-are-u-s-authorities-concerned-11594157084.

it may share user data with "corporate affiliates" and "third-party business partners."[80] Thus, even if TikTok refused a direct request from the Chinese government, U.S. lawmakers still fear that the Chinese government could wield its cybersecurity law to force "corporate affiliates," namely ByteDance, to comply with data requests.[81] TikTok has also allegedly exfiltrated facial recognition information from California to China,[82] and policy analysts fear that TikTok's algorithms favor pro-China content.[83] But both security experts and lawmakers are most concerned about TikTok's data collection practices and its ties to ByteDance, Tiktok's China-based parent company.[84]

Many of these same concerns pertain to WeChat. WeChat is known as the largest messaging platform in China, but it is much more than that: WeChat is an "all-purpose" app through which over a billion people shop, pay bills, read the news, and share photos.[85] For friends and loved ones in the United States, WeChat is one of the primary "digital bridges" that connects them with others in China.[86] But concerns of censorship, surveillance, and intimidation by the Chinese government ultimately led President Trump to issue the WeChat Order on August 6, 2020, prohibiting transactions through WeChat.[87]

One reason why the Executive Orders cannot meaningfully contribute to national security is that TikTok and WeChat are far from the only two companies with Chinese corporate affiliates operating in the United States.[88] And China is not the only country that may pose a threat to U.S. consumers' data privacy and security.[89] Furthermore, U.S. companies

80. Bobby Allyn, *Class-Action Lawsuit Claims TikTok Steals Kids' Data and Sends It to China*, NPR: ALL THINGS CONSIDERED, (Aug. 4, 2020, 1:39 PM ET), https://www.npr.org/2020/08/04/898836158/class-action-lawsuit-claims-tiktok-steals-kids-data-and-sends-it-to-china.

81. Ferek & Lin, *supra* note 66.

82. Kokas, *supra* note 7.

83. Helberg, *supra* note 77.

84. Ferek & Lin, *supra* note 66.

85. Mozur & Zhong, *supra* note 6.

86. *Id.*

87. WeChat Order, *supra* note 2; Paul Mozur, *Forget TikTok. China's Powerhouse App Is WeChat, and Its Power Is Sweeping*, N.Y. TIMES (Sept. 4, 2020), https://www.nytimes.com/2020/09/04/technology/wechat-china-united-states.html.

88. *See Chinese Investment in the United States Database*, PUB. CITIZEN, https://www.citizen.org/article/chinese-investment-in-the-united-states-database/ (last visited Dec. 19, 2021).

89. *See* Tiffany C. Li, *FaceApp Makes Today's Privacy Laws Look Antiquated*, ATLANTIC (July 20, 2019), https://www.theatlantic.com/ideas/archive/2019/07/faceapp-

collect the same data as TikTok and WeChat, if not more.[90] U.S. companies' data collection practices present significant privacy concerns to U.S. users because they do not adequately protect against foreign governments' access to sensitive user data through cyberattacks: "Combined with data gathered through hacks of Equifax, Marriott, Anthem and the Office of Personal Management, the Chinese government has a treasure trove of information to support intelligence-gathering activities for decades to come, regardless of [the TikTok and WeChat] bans."[91] The fact that President Trump invoked IEEPA to target TikTok and WeChat while the government failed to address U.S. companies' collection of user data suggests that "targeting a few big names merely distracts from the severity of the problem"[92] because these types of hacks will continue regardless of targeted bans on specific tech companies.[93]

Additionally, one of the primary concerns that the Executive Orders described is the threat that the Chinese government will wage disinformation campaigns through both TikTok and WeChat. Both Orders stated that the Chinese tech companies "reportedly censor[] content that the Chinese Communist Party deems politically sensitive . . . [and] may also be used for disinformation campaigns that benefit the Chinese Communist Party."[94] For example, WeChat has censored content related to human rights activists, religious groups, and as early as January 2020, key words pertaining to COVID-19.[95] Similarly, TikTok's algorithm has been accused of favoring pro-China content in the United States.[96] Although TikTok now allows political speech—unless the political speech contains "hate

reveals-huge-holes-todays-privacy-laws/594358/ (discussing privacy threats posed by the Russian-developed FaceApp among others).

90. Allyn, *supra* note 80 ("Experts said most smartphone apps collect and store just as much—or more—data as TikTok does.").

91. Kokas, *supra* note 7.

92. *Id.*

93. *See generally* Graham Webster, *App Bans Won't Make US Security Risks Disappear*, MIT TECH. REV. (Sept. 21, 2020), https://www.technologyreview.com/2020/09/21/1008620/wechat-tiktok-ban-china-us-security-policy-opinion/.

94. TikTok Order, *supra* note 2; WeChat Order, *supra* note 2.

95. *Coronavirus: Chinese App WeChat Censored Virus Content Since 1 Jan*, BBC NEWS (Mar. 4, 2020), https://www.bbc.com/news/world-asia-china-51732042; Eva Xiao, *China's WeChat Monitors Foreign Users to Refine Censorship at Home*, WALL ST. J. (May 8, 2020, 3:32 PM ET), https://www.wsj.com/articles/chinas-wechat-monitors-foreign-users-to-refine-censorship-at-home-11588852802.

96. Helberg, *supra* note 77.

speech"—it had previously censored political content to keep the video-sharing platform "as positive as possible."[97]

As the 2016 presidential election illustrated,[98] the threat posed by foreign disinformation campaigns is a topic of pressing importance that demands further scrutiny.[99] In the Internet's marketplace of ideas, there is an endless supply of foreign and domestic speech, and the source is often indiscernible.[100] But even if federal courts had ultimately upheld the Orders, it is unlikely that this would have made a cognizable difference in reducing the threat of Chinese disinformation campaigns in the United States. First, compared to Facebook and Twitter—where disinformation campaigns have the highest potential for success because of the platforms' reach—WeChat users constitute a small percentage of the population. Moreover, banning WeChat would be reminiscent of China's own blocking of websites such as Facebook, Twitter, and Google, and policy experts have questioned whether U.S. data security strategy should mirror China's censorship practices.[101] Second, disinformation campaigns waged on Facebook and Twitter suggest that the threat of disinformation will remain on TikTok regardless of whether it is owned by a U.S. or foreign company.

The United States certainly has a compelling interest in protecting national security,[102] and perhaps TikTok and WeChat do pose such a threat. But even if they do, the Executive Orders are incapable of meaningfully changing how companies harvest and store user data. TikTok and WeChat are only two of the many companies in the United States with potential ties to foreign governments, and U.S. companies have also failed to safeguard user data. Consequently, invoking IEEPA to target foreign mobile applications on a case-by-case will do little to protect national security and

97. Georgia Wells et al., *TikTok, Once an Oasis of Inoffensive Fun, Ventures Warily into Politics*, WALL ST. J. (July 8, 2020, 12:04 PM ET), https://www.wsj.com/articles/tiktok-ventures-warily-into-politicsand-finds-complications-11594224268.

98. *See, e.g.*, Joseph Thai, *The Right to Receive Foreign Speech*, 71 OKLA. L. REV. 269, 270–71 (2018).

99. See *id.* at 302–09 for a discussion of the First Amendment right to receive foreign speech and disinformation's impact on the marketplace of ideas.

100. *See generally id.* at 316–17 (discussing legislative and educational efforts to prevent the spread of misinformation and to require disclosures of the interested parties in online transactions and advertisements).

101. *See* Louise Matsakis, *Does TikTok Really Pose a Risk to US National Security?*, WIRED (July 17, 2020, 3:10 PM), https://www.wired.com/story/tiktok-ban-us-national-security-risk/ ("Outlawing TikTok would also mean the US would be participating in the same Chinese-style internet sovereignty tactics it has long criticized . . . .").

102. *See* Snepp v. United States, 444 U.S. 507, 509 n.3 (1980).

U.S. citizens' personal information. The successful legal challenges to the Orders further illustrate IEEPA's ill-fit use against foreign mobile applications.

2. Legal Challenges

In addition to IEEPA's inability to meaningfully reduce foreign mobile applications' threat to national security, executive orders targeting mobile applications pursuant to IEEPA are unlikely to survive legal challenges. Federal courts have enjoined the enforcement of both Orders, finding merit to challenges based on the First Amendment and an IEEPA provision banning the direct or indirect regulation of "personal communication[s]" and the exchange of "informational materials."[103]

In granting TikTok's motion for a preliminary injunction, the U.S. District Court for the District of Columbia recognized that the TikTok Order likely exceeded the President's IEEPA powers because it might have indirectly regulated "personal communication[s]" or the exchange of "information or informational materials."[104] IEEPA sections 1702(b)(1) and 1702(b)(3) specifically restrict direct or indirect regulation of these exchanges.[105] While the district court's grant of a preliminary injunction was not a ruling on the merits, the challenge would likely apply to any use of IEEPA to target a popular tech company through which users exchange messages or share content.

The U.S. WeChat Users Alliance (the plaintiff that challenged the WeChat Order) also obtained a preliminary injunction, but on different grounds. In granting the preliminary injunction, the U.S. District Court for the Northern District of California concluded that the U.S. WeChat Users Alliance presented "serious questions going to the merits of their First Amendment claim" because the government's measures "effectively eliminate[d] the plaintiffs' key platform for communication, slow[ed] or eliminate[d] discourse, and [was] the equivalent of censorship of speech or a prior restraint on it."[106] The court noted that there is not another viable platform because WeChat is the only option for many Chinese speakers with limited English proficiency.[107]

103. 50 U.S.C. § 1701.
104. TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 83 (D.D.C. 2020).
105. *Id.* at 81, 83.
106. U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912, 926 (N.D. Cal. 2020).
107. *Id.* at 927.

The court further concluded that even if the Order were a content-neutral time-place-or-manner restriction, it would likely fail even under intermediate scrutiny.[108] A content-neutral restriction must be narrowly tailored to serve a significant government interest, be "justified without reference to the content of the regulated speech," and provide "ample alternative channels for communication."[109] The regulation does not need to be the least restrictive means, "[b]ut the government still may not regulate expression in such a manner that a substantial portion of the burden on speech does not serve to advance its goals."[110] In granting the preliminary injunction, the district court concluded that while the government's national-security interest was significant, the Order was likely not narrowly tailored because a substantial portion of the restriction burdened speech in a way that might not have advanced the government's interest.[111] Rather than implementing an all-out ban, the government could have burdened substantially less speech by prohibiting WeChat usage on government devices or "taking other steps to address data security."[112]

These legal challenges demonstrate that IEEPA cannot be used as a tool to ban foreign mobile applications in the United States. But even if courts had ultimately upheld the Orders, the threat to national security will persist until there is a more comprehensive and nuanced approach to protecting data privacy.

II. Federal Data Privacy Legislation Is a Superior Alternative to IEEPA

The threat posed by foreign governments' access to consumers' personal data is heightened by the business model that makes it possible: advertisement-based websites and applications that extract and monetize personal data.[113] This personal data includes information such as page views, searches, physical locations, browsing history, device IDs, and user emails.[114] Many mobile applications do not charge a user fee, but these services are not really free: "We don't pay for the product because we *are*

108. *Id.* at 927–28.

109. Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (quoting Clark v. Cmty. for Creative Non-Violence, 468 U.S. 288, 293 (1984)).

110. McCullen v. Coakley, 573 U.S 464, 486 (2014) (internal quotation marks omitted) (quoting *Ward*, 491 U.S. at 799).

111. *U.S. WeChat Users All.*, 488 F. Supp. 3d at 927.

112. *Id.*

113. *See generally* Cook, *supra* note 28.

114. *See* Evelyn Mary Aswad, *Losing the Freedom to Be Human*, 52 COLUM. HUM. RTS. L. REV. 306, 318–19 (2020).

the product."[115] While individual pieces of data may be "harmless enough on [their] own," they are "carefully assembled, synthesized, traded, and sold."[116] As Apple CEO Tim Cook has warned, "This is surveillance."[117] The routine and pervasive practice of data harvesting by technology companies has been increasingly recognized as an incursion into people's right to privacy[118] and even an interference with people's right to hold opinions without interference.[119]

Part II discusses the pressing need for federal data privacy legislation. While enacting data privacy legislation would not eliminate national security issues posed by foreign mobile applications operating in the United States, it would be an important step towards safeguarding privacy and protecting national security interests. Section II.A. begins by situating data privacy in the context of international human rights. Section II.B then examines data privacy bills before the 117th Congress and recommends improvements. Any of these bills, several of which share similarities with the European GDPR and the California Consumer Privacy Act, would be a monumental step forward for the United States in protecting user data. But each bill omits key features that would better safeguard U.S. citizens' right to privacy and protect national security, most notably a provision that would regulate international data transfers.

A. Privacy Is an Internationally Recognized Human Right

The U.S. Supreme Court has recognized that due process provides for an individual's right to privacy in certain contexts.[120] But because the

115. Geoffrey A. Fowler, *What If We Paid for Facebook—Instead of Letting It Spy on Us for Free?*, WASH. POST (April 5, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/05/what-if-we-paid-for-facebook-instead-of-letting-it-spy-on-us-for-free/.

116. Sam Schechner & Emre Peker, *Apple CEO Condemns 'Data-Industrial Complex'*, WALL ST. J. (Oct. 24, 2018, 11:41 AM ET), https://www.wsj.com/articles/apple-ceo-tim-cook-calls-for-comprehensive-u-s-privacy-law-1540375675.

117. *Id.*

118. *See, e.g.*, Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355 (2015); Kalinda Basho, Comment, *The Licensing of Our Personal Information: Is It a Solution to Internet Privacy?*, 88 CAL. L. REV. 1507 (2000).

119. Aswad, *supra* note 114, at 363.

120. Griswold v. Connecticut, 381 U.S. 479, 500 (1965) (Harlan, J., concurring) (finding a right to privacy under the Fourteenth Amendment); Roe v. Wade, 410 U.S. 113, 153 (1973) (finding that the right to privacy as derived from the Fourteenth Amendment encompasses a woman's right to an abortion); Lawrence v. Texas, 539 U.S. 558, 578 (2003) (finding that the Fourteenth Amendment extends the right of privacy to private sexual relationships).

extraction and monetization of personal data is a global practice, this Comment examines data privacy in the context of existing international human rights frameworks. Furthermore, the United States has endorsed a voluntary framework, the U.N. Guiding Principles on Business and Human Rights ("UNGPs"), which provides minimum standards for companies that face human rights issues and calls on governments to take appropriate legislative steps to protect internationally recognized human rights as enshrined in U.N. instruments.[121]

In the U.N. human rights system, the right to privacy is commemorated in the Universal Declaration of Human Rights ("UDHR"). The U.N. General Assembly unanimously adopted the UDHR in 1948 in pursuit of establishing an "international Bill of Rights."[122] While not legally binding, the UDHR provided a framework for understanding internationally recognized human rights, and through its thirty articles, the UDHR laid a foundation for future U.N. documents and international human rights treaties.[123]

Article 12 of the UDHR provides that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[124] The UDHR also contains a general limitations clause that applies to each right:

> In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.[125]

---

121. Aswad, *supra* note 114, at 312–13; U.S. DEP'T OF STATE, U.S. GOVERNMENT APPROACH ON BUSINESS AND HUMAN RIGHTS 4 (2013), https://kr.usembassy.gov/wp-content/uploads/sites/75/2017/04/dwoa_USG-Approach-on-Business-and-Human-Rights-updatedJune2013.pdf ("The U.S. government encourages stakeholders to treat the Guiding Principles as a 'floor' rather than a 'ceiling' for addressing issues of business and human rights, and to recognize that implementing the Guiding Principles should be a continuous process.").

122. SEAN D. MURPHY, PRINCIPLES OF INTERNATIONAL LAW 401–02 (3d ed. 2018).

123. *Id.* at 402.

124. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

125. *Id.* art. 29(2).

But because the UDHR is not legally binding, the U.N. Commission on Human Rights set out to conclude a legally binding treaty that would incorporate the UDHR's principles.[126] This led to the adoption of the International Covenant on Civil and Political Rights ("ICCPR").[127] The ICCPR entered into force in 1976, and as of 2022, the treaty has 173 state parties, including the United States.[128]

Similar to article 12 of the UDHR, article 17 of the ICCPR addresses the right to privacy. Specifically, it provides that

> [n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation [and that] [e]veryone has the right to the protection of the law against such interference or attacks.[129]

Furthermore, state parties to the ICCPR "undertake[] to respect and to ensure to all individuals within [their] territory and subject to [their] jurisdiction the rights recognized in the present Covenant."[130]

Certainly, the UDHR and ICCPR did not envision the rise of twentieth century data collection practices and the issues they pose, let alone the national security and privacy threats posed by mobile application companies such as TikTok and WeChat. And countries have applied the UDHR and ICCPR's right to privacy in different ways.[131] But while the UDHR and the ICCPR did not envision the pervasive harvesting and monetization of personal data, recent U.N. resolutions have demonstrated that the right to privacy enshrined in both the UDHR and ICCPR applies to digital privacy.[132] These resolutions have "confirm[ed] the tendency to anchor data protection in the context of international human rights law."[133]

---

126. MURPHY, *supra* note 122, at 404.

127. *Id.*

128. Aswad, *supra* note 114, at 327; *International Covenant on Civil and Political Rights*, UNITED NATIONS TREATY COLLECTION, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en (last visited Jan. 2, 2022).

129. International Covenant on Civil and Political Rights, art. 17(1)–(2), *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171, 177 (entered into force Mar. 23, 1976). It is important to note that not all government invasions of privacy would violate ICCPR article 19. To violate the article, the invasion of privacy must either be "arbitrary" or "unlawful." *Id.*

130. *Id.* art. 2(1).

131. *See* Joshua Blume, Note, *A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR*, 49 GEO. J. INT'L L. 1425, 1428 (2018).

132. U.N. Resolution 68/167 provides in part:

While the UDHR and treaties such as the ICCPR generally apply to nation-states, there is another international framework that applies to private companies. The United States has endorsed this framework—the UNGPs—describing it "as a minimum standard for American companies."[134] The UNGPs call for companies to respect human rights as memorialized in U.N. instruments, including the UDHR and ICCPR.[135] And as U.N. developments have shown, the concept of privacy in the UDHR and ICCPR includes data privacy.[136]

The UNGPs also require governments to take appropriate legislative steps to protect human rights. Principle 1 of the UNGPs provides that governments "must protect against human rights abuse" by corporations within their territory.[137] This protection "requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, *legislation*, regulations and adjudication."[138] But when it comes to regulating corporate abuse of the right to data privacy, U.S. legislation has "significantly lagged behind" the rest of the world.[139] In fact, the United States is one of the only economically developed nations without a

---

> [T]he rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern . . . .

G.A. Res. 68/167 at pmbl. (Dec. 18, 2013).

133. Francesca Bignami & Giorgio Resta, *Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance* (G.W. L. Sch. Pub. L. & Legal Theory Paper No. 2016-67), https://ssrn.com/abstract=3043771.

134. Aswad, *supra* note 114, at 312.

135. *Id.* at 313 n.12; U.N. Special Representative of the Secretary-General on Human Rights and Transnational Corporations and Other Business Enterprises, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, princ. 12, U.N. DOC. A/HRC/17/31 (Mar. 21, 2011) [hereinafter *UNGPs*].

136. G.A. Res. 68/167132.

137. *UNGPs*, *supra* note 135, at princ. 1.

138. *Id.* (emphasis added).

139. Samer Kamal, *Where Does the U.S. Rank in the Global Data Privacy Landscape?*, CPO MAG. (Apr. 24, 2020), https://www.cpomagazine.com/data-privacy/where-does-the-u-s-rank-in-the-global-data-privacy-landscape/.

comprehensive national consumer data privacy law.[140] The lack of a national data privacy law "has left Americans at the mercy of digital services that have every reason to exploit our personal information and little incentive to safeguard it."[141]

In addition to requiring governments to take appropriate legislative action to protect human rights, the UNGPs also state that companies have a responsibility to respect human rights, including through conducting human rights due diligence assessments.[142] This means companies should "assess[] actual and potential human rights impacts, integrat[e] and act[] upon the findings, track[] responses, and communicat[e] how impacts are addressed."[143] But the technology companies whose business models are based on harvesting and monetizing personal information[144] do not conduct human rights impact assessments.[145] Perhaps if technology companies had implemented the UNGPs' human rights due diligence requirement before building business models based on harvesting personal data, the right to privacy would be better respected in the digital sphere today.

The UNGPs should both compel and inform the creation of a national consumer data privacy law because the UNGPs call on governments to take appropriate legislative steps to protect human rights, and U.S. companies have not respected the right to data privacy or conducted human rights due diligence. Section II.B compares existing international and state data privacy frameworks to four data privacy bills that are before the 117th Congress, recommending further measures that a federal data privacy law should include to better safeguard U.S. citizens' personal information and protect national security.

B. Federal Data Privacy Legislation Will Better Safeguard Human Rights and National Security

Federal data privacy legislation would not only protect U.S. citizens' right to data privacy but also benefit the U.S. government's national

140. *See generally* Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?*, N.Y. TIMES (Nov. 2, 2019), https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html (stating that instead of a national data privacy law, "Americans have to rely on the Federal Trade Commission, an overstretched agency with limited powers, to police privacy as a side hustle").

141. *Id.*

142. *UNGPs*, *supra* note 135, at princ. 17–21.

143. *Id*. at princ. 17.

144. Aswad, *supra* note 114, at 310.

145. *Id.* at 366.

security interests.[146] Properly designed national legislation would provide "security authorities with the information they need to feel confident that specific apps do not pose a privacy or security risk" and "help ensure that freedom of expression and privacy are honored across our connected lives."[147] As awareness of the national security risks posed by foreign actors' access to U.S. citizens' data has grown, calls for a federal data privacy bill have received more bipartisan support.[148] And Chinese companies' increased access to the U.S. market—most vividly illustrated by TikTok's precipitous rise in popularity—has intensified the desire to pass federal legislation.[149]

While passing a federal data privacy law would not eliminate all threats related to data privacy and national security,[150] it would be a meaningful step in the right direction for numerous reasons. For example, a national law would harmonize the existing patchwork of state consumer privacy laws.[151] The existing patchwork of state laws adds compliance costs and constraints on operability across state lines, making U.S. companies less competitive on a global scale[152] while failing to adequately protect consumers or address national security threats.[153] A federal data privacy law

146. *See, e.g.*, Claudia Biancotti, *For the United States, More Digital Privacy Would Mean More National Security*, PETERSON INST. FOR INT'L ECON.: REALTIME ECON. ISSUES WATCH (Apr. 10, 2019, 5:30 PM), https://www.piie.com/blogs/realtime-economic-issues-watch/united-states-more-digital-privacy-would-mean-more-national ("Most worries about foreign entities prying into American lives could be assuaged by strengthening everyday digital rights, a move with benefits beyond security."); Carrie Cordero, *The National Security Imperative of Protecting User Data*, CTR. FOR NEW AM. SEC. (Apr. 24, 2019), https://www.cnas.org/publications/commentary/the-national-security-imperative-of-protecting-user-data ("Policy debates over national security legal authorities, like surveillance, have traditionally pitted those favoring national security equities against those favoring privacy equities. The choice is a false one.").

147. Webster, *supra* note 93.

148. Robert D. Williams, *To Enhance Data Security, Federal Privacy Legislation Is Just a Start*, BROOKINGS INST.: TECHSTREAM (Dec. 1, 2020), https://www.brookings.edu/techstream/to-enhance-data-security-federal-privacy-legislation-is-just-a-start/.

149. *Id.*

150. *Id.*

151. *See* WILSON C. FREEMAN, CONG. RSCH. SERV., LSB10213, CALIFORNIA DREAMIN' OF PRIVACY REGULATION: THE CALIFORNIA CONSUMER PRIVACY ACT AND CONGRESS 1 (2018), https://fas.org/sgp/crs/misc/LSB10213.pdf.

152. Christine S. Wilson, Comm'r, FTC, A Defining Moment for Privacy: The Time Is Ripe for Federal Privacy Legislation, Remarks at the Future of Privacy Forum 7–8 (Feb. 6, 2020), https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf.

153. *Id.* at 7.

would create a unified, predictable framework for businesses operating in the U.S. market. Additionally, a federal data privacy law could address discrimination risks posed by the aggregation and use of consumer profiles,[154] enshrine "baseline privacy as a core U.S. value,"[155] and promote innovation through "clearly defined and consistently applied rules."[156]

But there are numerous questions surrounding the scope of a federal data privacy law, primarily related to whether it would preempt existing state laws, whether it would provide a private right of action, and how it would be enforced.[157] Policy analysts have challenged the implementation of a federal data privacy law on economic grounds.[158] And while it is important to include technology companies in the debate, any legislation will likely receive opposition from powerful stakeholders whose business models revolve around harvesting user data.[159] So, rather than adding to the debate over preemption, a private right of action, and enforcement, this section examines key features of the GDPR and U.S. state data privacy approaches that should inform a federal law. In particular, a federal law should incorporate the strong data privacy rights of the GDPR and U.S. state laws, as well as elements of the GDPR's regulation of cross-border data transfers.

154. Peter M. Lefkowitz, *Why America Needs a Thoughtful Federal Privacy Law*, N.Y. TIMES (June 25, 2019), https://www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html.

155. Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Finally Pass a Baseline Privacy Law*, BROOKINGS INST.: TECHTANK (Jan. 14, 2021), https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/.

156. Harper Neidig, *51 Major CEOs Ask Congress for Federal Privacy Law Blocking State Rules*, HILL (Sept. 10, 2019, 2:23 PM EDT), https://thehill.com/policy/technology/460737-51-major-ceos-urge-congress-to-pass-privacy-law-blocking-state-data.

157. STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., IF11207, DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION (2019), https://crsreports.congress.gov/product/pdf/IF/IF11207.

158. ALAN MCQUINN & DANIEL CASTRO, INFO. TECH. & INNOVATION FOUND., THE COSTS OF AN UNNECESSARILY STRINGENT FEDERAL DATA PRIVACY LAW 1 (Aug. 2019), https://itif.org/sites/default/files/2019-cost-data-privacy-law.pdf.

159. Webster, *supra* note 93 ("There is well-organized opposition to enacting serious privacy rules in the United States, and those opponents can far outspend all existing efforts to make real progress on this issue.").

1. The European Union's General Data Protection Regulation

The GDPR took effect on May 25, 2018, and has since fueled debate over U.S. data privacy policies.[160] Through the GDPR, the EU provides "the world's toughest rules to protect people's online data" and is a "sharp divergence from the United States, which has taken little action over the years in regulating the tech industry."[161] The law is grounded in the EU's stance that privacy of communications and personal data is a fundamental human right.[162]

The GDPR limits how businesses can process personal data and has an "aggressive extraterritorial scope."[163] It applies to any business that processes personal data of individuals in the EU,[164] regardless of the business's location or the individual's country of citizenship.[165] "Personal data" is broadly defined as "any information relating to an identified or identifiable natural person," and an "identifiable natural person" is defined as one who can be directly or indirectly identified "by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[166]

The GDPR also created data protection requirements that give individuals in the EU certain rights related to how companies process their personal data. These rights include the following:

- the "right to be forgotten," which allows individuals to request companies delete all their personal data;

160. RACHEL F. FEFER & KRISTIN ARCHICK, CONG. RSCH. SERV., IF10896, EU DATA PROTECTION RULES AND U.S. IMPLICATIONS (2020), https://fas.org/sgp/crs/row/IF10896.pdf.

161. Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

162. FEFER & ARCHICK, *supra* note 160; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR] ("The protection of natural persons in relation to the processing of personal data is a fundamental right.").

163. Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 378 (2019).

164. *Id.* at 377.

165. Stuart L. Pardau, *The California Consumer Privacy Act: Towards A European-Style Privacy Regime in the United States?*, 23 J. TECH. L. & POL'Y 68, 86 n.100 (2018).

166. GDPR, *supra* note 162, art. 4(1).

- the "right to object," which allows individuals to object to certain uses of their personal data;
- the "right to rectification," which allows individuals to request companies correct incorrect or incomplete personal data;
- the "right of portability," which allows individuals to request companies transfer their personal data to another company;
- the "right of access," which allows individuals to learn what personal data companies have collected and how companies use that data; and
- the "right to be notified," which requires companies to notify individuals of a breach within seventy-two hours of gaining knowledge of the breach.[167]

In addition to providing these rights to individuals in the EU, the GDPR regulates the flow of personal data from the EU to third countries (any country outside the EU and the European Economic Area) and international organizations.[168] Under the GDPR, businesses may transfer personal data to third countries or international organizations that provide adequate protection to that data.[169] The European Commission, the EU's primary executive body, is tasked with making these "adequacy decisions" concerning third countries and international organizations' level of data protection.[170] In determining whether a third country or international organization provides adequate protection, the Commission considers various factors:

> the rule of law, respect for human rights and fundamental freedoms, relevant legislation, . . . the access of public authorities to personal data, . . . data protection rules, . . . rules for the onward transfer of personal data to another third country or international organisation . . . as well as effective and enforceable data subject rights and effective administrative and

167. Rustad & Koenig, *supra* note 163, at 377.

168. GDPR, *supra* note 162, art. 44; *Data Transfer to Third Countries*, GDPR INFORMER (Sept. 5, 2017), https://gdprinformer.com/gdpr-articles/data-transfers-third-countries.

169. *Id.*

170. W. Gregory Voss, *Cross-Border Data Flow, the GDPR, and Data Governance*, 29 WASH. INT'L L.J. 485, 507 (2020); James McBride, *How Does the European Union Work?*, COUNCIL ON FOREIGN RELS. (Apr. 17, 2020, 8:00 AM EST), https://www.cfr.org/backgrounder/how-does-european-union-work.

> judicial redress for the data subjects whose personal data are being transferred.[171]

As of January 2022, the Commission has determined that fourteen countries provide adequate protection.[172] The United States is not one of them.[173]

Absent an adequacy determination, businesses may transfer personal data out of the EU through other legal means. The most commonly used method is through Standard Contractual Clauses.[174] Standard Contractual Clauses are Commission-approved contract provisions for use when businesses transfer data to a third country or international organization that does not provide adequate legal protection to personal data.[175] Businesses that export personal data from the EU can include these pre-approved clauses to engage in cross-border data transfers to third countries and international organizations that have not earned adequacy determinations.[176] A key requirement of these Standard Contractual Clauses is that they allow individuals to directly enforce their GDPR rights against both the businesses transferring and receiving the personal data.[177]

But these pre-approved Standard Contractual Clauses are not without a critical weakness: they are unable to prevent a third country's government from lawfully requesting access to the transferred personal data, including requests related to national security.[178] So while the European Court of Justice ("ECJ") has upheld the validity of Standard Contractual Clauses, it

171. GDPR, *supra* note 162, art. 45(2)(a).

172. *Adequacy Decisions: How the EU Determines If a Non-EU Country Has an Adequate Level of Data Protection*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions (last visited Jan. 13, 2021).

173. *See id.* The European Union and United States had previously negotiated an agreement called the Privacy Shield, under which thousands of small and medium-sized enterprises could transfer data from the EU to the United States. *See* Nigel Cory et al., *'Schrems II': What Invalidating the EU-U.S. Privacy Shield Means for Transatlantic Trade and Innovation*, INFO. TECH. & INNOVATION FOUND., Dec. 2020, at 1 https://itif.org/sites/default/files/2020-privacy-shield.pdf. But the European Court of Justice has since invalidated the EU-U.S. Privacy Shield in its *Schrems II* decision, which means U.S. businesses will likely turn to another GDPR mechanism for data transfers—standard contractual clauses approved by the European Commission. *Id.* at 2.

174. NIGEL CORY ET AL., INFO. TECH. & INNOVATION FOUND., THE ROLE AND VALUE OF STANDARD CONTRACTUAL CLAUSES IN EU-U.S. DIGITAL TRADE 1 (Dec. 2020), https://itif.org/sites/default/files/2020-standard-contractual-clauses.pdf.

175. *Id.*

176. *Id.* at 3.

177. *Id.*

178. *Id.*

concluded that "[i]f compliance with the laws of the receiving country requires the data importer to forego adequate protections regardless of the safeguards in place, then 'the controller or processor . . . [is] required to suspend or end the transfer of personal data to the third country concerned.'"[179] The ECJ stated that to "ensure compliance with the level of protection required under EU law," the Standard Contractual Clauses may require "supplementary measures."[180] The ECJ, however, did not define supplementary measures.[181] Thus, at least under the GDPR, the future of Standard Contractual Clauses—and consequently all data transfers from the EU to countries not included in the fourteen that the Commission has deemed to provide adequate legal protection—is uncertain.[182]

While the workability and effects of the GDPR are still unfolding in the ECJ and the global market, its robust protection of personal data has inspired the adoption of similar data privacy laws in other countries. One such law is the California Consumer Privacy Act ("CCPA") and its amendment, the California Privacy Rights Act ("CPRA").[183] Other states, including Oklahoma, have introduced bills that largely mirror the California law but apply to different categories of businesses and provide different levels of rights and protections for each state's consumers.

2. State Data Privacy Approaches: California and Oklahoma

The California State Constitution recognizes privacy as an inalienable right[184] and is the only state constitution to do so.[185] This inalienable right to privacy underpins the CCPA, which went into effect on January 1, 2020.[186]

The CCPA largely restricts businesses' collection and sale of consumers' "personal information."[187] The law currently applies to for-profit businesses

179. *Id.* at 6 (second alteration in original).

180. *Id.* at 6–7.

181. *Id.* at 6.

182. *See* Voss, *supra* note 170, at 516 ("[T]he use of standard contract clauses as an appropriate safeguard has . . . come under attack.").

183. CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2021) (incorporating Act of Oct. 11, 2019, ch. 757, CAL. CIV. CODE §§ 1798.100, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.140, 1798.145, 1798.150, 1798.185).

184. CAL. CONST. art. I, § 1.

185. Mark Smith, *Analysis: California Privacy Reboot Puts Rights in Spotlight*, BLOOMBERG L. (Jan. 15, 2021, 9:05 AM), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-california-privacy-reboot-puts-rights-in-spotlight.

186. *See* CAL. CIV. CODE §§ 1798.100–1798.199.100 (noting the effective date for California Privacy Rights Act amendments as January 1, 2021).

187. FREEMAN, supra note 151, at 2.

that satisfy one of three criteria: (1) earn more than $25 million in annual gross revenue; (2) "[a]lone or in combination, annually buy[], receive[] for the business's commercial purposes, sell[], or share[] for commercial purposes . . . the personal information of 50,000 or more consumers, households, or devices"; or (3) "[d]erive[] 50 percent or more of [their] annual revenues from selling consumers' personal information."[188] The CCPA defines "consumers" as natural persons who are California residents[189] and "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[190]

The CCPA, which is modelled after the GDPR, was "crafted to protect individual privacy as a fundamental right."[191] The CCPA thus provides California consumers with several rights, including (1) the "right to know," (2) the "right to opt out," and (3) the "right to delete."[192] The "right to know" allows consumers to know the information that business have collected about them during the past twelve months, the "right to opt out" allows consumers to prevent businesses from selling their personal information, and the "right to delete," as the name implies, allows consumers to request that a business delete any personal information it has collected from them.[193] The CCPA also provides that a business may not "discriminate against a consumer by 'denying goods or services' or by 'charging different prices or rates' to consumers who exercise their rights under the CCPA."[194] Businesses must inform consumers about these rights

188. CAL. CIV. CODE § 1798.140(c)(1). With the passing of the CPRA, California increased the requirement under § 1798.140(c)(1)(B) to 100,000 or more California residents, and the covered personal information no longer includes "devices." Stacey Gray et al., *California's Prop 24, The "California Privacy Rights Act," Passed. What's Next?*, FUTURE OF PRIV. F. (Nov. 4, 2020), https://fpf.org/blog/californias-prop-24-the-california-privacy-rights-act-passed-whats-next/.

189. CAL. CIV. CODE § 1798.140(g).

190. *Id.* § 1798.140(v)(1).

191. Catherine Barrett, *Are the EU GDPR and the California CCPA Becoming the De Facto Global Standards for Data Privacy and Protection?*, SCITECH LAW., Spring 2019, at 24, 28.

192. FREEMAN, supra note 151, at 3.

193. *Id.*

194. *Id.*

and provide methods to exercise these rights without cost.[195] Unlike the GDPR, however, the CCPA does not regulate cross-border data transfers.[196]

In November 2020, California passed the CPRA, which both modified these rights under the CCPA and created new ones.[197] These modifications to the CCPA include the following:

- expanding the right to opt out of a *sale* to the right to opt out of a sale or *sharing* of personal information;[198]
- expanding the right to opt out to include opting out of "automated decision-making technology";[199]
- expanding the right to know by eliminating the CCPA's twelve-month limitation;[200]
- expanding the right to delete to require service providers and third parties to cooperate with businesses to delete personal information;[201]
- creating a right for consumers to correct inaccurate personal information about the consumer and requiring businesses to inform consumers about this right;[202]
- creating a right for consumers to limit the sale or internal use of "sensitive information," which includes "information concerning

195. *Id.*

196. Carol A. F. Umhoefer, *CCPA vs. GDPR: The Same, Only Different*, DLA PIPER: INTELL. PROP. & TECH. NEWS (Apr. 11, 2019), https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr/.

197. Gray et al., *supra* note 188; Cameron F. Kerry & Caitlin Chin, *By Passing Proposition 24, California Voters Up the Ante on Federal Privacy Law*, BROOKINGS INST.: TECHTANK (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/ (discussing the ways in which the CPRA modified and expanded rights under the CCPA).

198. Gray et al., *supra* note 188.

199. Colleen Theresa Brown et al., *California Privacy Law Overhaul – Proposition 24 Passes*, SIDLEY AUSTIN LLP: DATA MATTERS (Nov. 4, 2020), https://datamatters.sidley.com/california-privacy-law-overhaul-proposition-24-passes.

200. Gray et al., *supra* note 188.

201. F. Paul Pittman & Kyle Levenberg, *Before the Dust Settles: The California Privacy Rights Act Ballot Initiative Modifies and Expands California Privacy Law*, WHITE & CASE (Nov. 13, 2020), https://www.whitecase.com/publications/alert/dust-settles-california-privacy-rights-act-ballot-initiative-modifies-and.

202. Gray et al., *supra* note 188.

health, race and ethnicity, sexual orientation, precise geolocation, and more;"[203] and

- creating a new data minimization and purpose requirement[204] that (1) limits businesses' collection of personal information to information that is reasonably necessary and proportionate to the reasons the business collected the information and (2) prohibits processing that information for a purpose incompatible with those reasons.[205]

Most interestingly, the CPRA establishes the California Privacy Protection Agency.[206] The Agency has the authority to promulgate rules, enforce the amended CCPA, and require businesses to conduct cybersecurity audits and risk assessments for the Agency's chief privacy auditor to ensure compliance with the CPRA.[207] The Agency also plays a broader educational role by promoting "public awareness and understanding of the risks, rules, responsibilities, safeguards, and rights in relation to the collection, use, sale and disclosure of personal information."[208] Given California's far-reaching impact on the global technology market, the Agency will be a key privacy regulator around the world.[209]

Since California passed the CCPA in 2018, multiple states have proposed similar legislation to protect consumer data privacy.[210] Oklahoma is one such state.[211] Introduced in September of 2021,[212] the Oklahoma

203. *Id.*

204. This provision mirrors the GDPR. *See* GDPR, *supra* note 162, recitals ¶¶ 49, 50 (limiting the processing of personal data to "the extent strictly necessary and proportionate for the purposes of ensuring network and information security" and "for purposes other than those for which the personal data were initially collected").

205. Gray et al., *supra* note 188.

206. Pittman & Levenberg, *supra* note 201.

207. *See id.*

208. Lydia de la Torre & Glenn Brown, *What Is the California Privacy Protection Agency?*, IAPP (Nov. 23, 2020), https://iapp.org/news/a/what-is-the-california-privacy-protection-agency/.

209. *Id.*

210. Taylor Kay Lively, *US State Privacy Legislation Tracker*, IAPP: RESOURCE CTR. (Feb. 17, 2022), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

211. Oklahoma Computer Data Privacy Act of 2022, H.B. 2968, 58th Leg., 2d Sess. (Okla. 2022).

212. David Stauss et al., *2022 Oklahoma Computer Data Privacy Act Filed*, HUSCH BLACKWELL: BYTE BACK (Sept. 9, 2021), https://www.bytebacklaw.com/2021/09/2022-oklahoma-computer-data-privacy-act-filed/.

Computer Data Privacy Act of 2022 ("OCDPA") would apply to certain for-profit businesses that conduct business in the state, collect consumers' personal information, and satisfy at least one of the following thresholds: (1) receive $10 million in annual gross revenues; (2) receive the personal information of twenty-five thousand consumers per year; or (3) derive at least fifty percent of annual revenue from sharing personal information.[213] The Act defines a "consumer" as an Oklahoma resident[214] and "personal information" as any information that "identifies or could reasonably be linked, directly or indirectly, with a particular consumer, household, or consumer device."[215]

Like the CCPA,[216] the OCDPA provides Oklahomans with the right to know,[217] the right to opt out,[218] and the right to delete.[219] And like the CPRA,[220] the OCDPA creates a right to correct[221] and includes a data minimization requirement that limits businesses to collecting and sharing with third parties only personal information "that is reasonably necessary to provide a good or service to a consumer who has requested the same or is reasonably necessary for security purposes or fraud detection."[222] Significantly, the "monetization of personal information shall never be considered reasonably necessary for any purpose."[223] Unlike the CCPA, however, the OCDPA does not define or provide a right to limit the use of "sensitive personal information."[224]

If passed, the Oklahoma law would provide residents with data privacy rights similar to those under the CCPA and CPRA, but it would also further complicate the existing patchwork of state laws that have sought to fill the void of a federal data privacy framework. Importantly, state laws do not

213. Oklahoma Computer Data Privacy Act of 2022, H.B. 2968 § 3(3)(a). "Share" is broadly defined as "renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose." *Id.* § 3(17).

214. *Id.* § 3(6).

215. *Id.* § 3(13).

216. *See supra* note 192 and accompanying text.

217. Oklahoma Computer Data Privacy Act of 2022, H.B. 2968 § 8.

218. *Id.* § 6(C).

219. *Id.* § 7(A).

220. *See supra* notes 202 and 205 and accompanying text.

221. Oklahoma Computer Data Privacy Act of 2022, H.B. 2968 § 9.

222. *Id.* § 6(A).

223. *Id.*

224. *Compare id.* § 3(13), *with* CAL. CIV. CODE § 1798.140(ae).

regulate international data transfers, and varying state laws contribute to added compliance challenges for businesses that collect consumers' personal information across different states, further illustrating the need for a comprehensive U.S. federal law.

3. Recommendations for a U.S. Federal Data Privacy Law

The GDPR, CCPA, and the growing number of state privacy laws[225] have informed the debate in Congress over a U.S. federal data privacy law, and the bills currently before the 117th Congress incorporate their provisions to varying degrees. Many of the bills' strengths lie in providing strong, affirmative data privacy rights that largely mirror the rights provided in the GDPR and CCPA/CPRA. But to adequately protect Americans' data privacy and reduce national security risks from foreign companies operating in the United States, such as TikTok and WeChat, a U.S. federal data privacy law will need to resist overly restricting cross-border data flow while protecting U.S. citizens' personal data from foreign governments when it leaves U.S. borders. Cross-border data flow is "essential to economic growth in the digital age,"[226] but foreign governments' access to U.S. citizens' data poses a national security risk.[227] A federal data privacy law must therefore strike a balance between these competing interests, ensuring that cross-border data flow does not jeopardize national security.

The data privacy bills before the 117th Congress provide an opportunity for the United States to better protect consumers' privacy and national security interests. One such bill, the Information Transparency and Personal Data Control Act, calls for the United States to "develop a balanced, high-

225. *The Growth of State Privacy Legislation*, IAPP: RESOURCE CTR. (Nov. 2021), https://iapp.org/resources/article/the-growth-of-state-privacy-legislation-infographic/ (tracking the rapid growth of state privacy legislation from 2018 to 2021).

226. Joshua P. Meltzer & Peter Lovelock, *Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia*, BROOKINGS INST. (Mar. 20, 2018), https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/ (discussing the economic dangers of data localization).

227. *See* Samm Sacks, *Data Security and U.S.-China Tech Entanglement*, LAWFARE (Apr. 2, 2020, 8:00 AM), https://www.lawfareblog.com/data-security-and-us-china-tech-entanglement (arguing for a "risk-based approach" to restricting access to U.S. personal data); H. Jacqueline Brehmer, Note, *Data Localization: The Unintended Consequences of Privacy Litigation*, 67 AM. U. L. REV. 927 (2018) (discussing the effects of data localization on privacy and national security).

standard digital privacy framework that complements global standards."[228] Providing affirmative data privacy rights similar to those under the GDPR and CCPA/CPRA, the Act would give consumers the right to access and correct personal data,[229] provide opt-in and opt-out rights for certain personal information,[230] and mandate "reasonable limits on the personal data that companies collect and retain."[231] The Act would also require privacy audits every two years by a "qualified, objective, independent third party."[232]

Significantly, like the CPRA, the Information Transparency and Personal Data Control Act defines certain categories of information as "sensitive personal information."[233] The bill broadly defines "sensitive personal information" to include information such as financial account numbers, health information, genetic data, geolocation information, content of personal communications, sexual orientation, religion, immigration status, and browsing history.[234] The definition does not include de-identified information, information related to employment, or publicly available information.[235]

Under the Information Transparency and Personal Data Control Act, before an individual's sensitive personal information may be "collected, transmitted, stored, process[ed], sold, or otherwise shared" by a controller,[236] the individual must "provide affirmative, express consent."[237] Consumers' opt-in consent is thus a requirement for the collection and use of all sensitive personal data, as well as for sharing sensitive personal information with third parties.[238] While the bill broadly defines "third parties," it does not explicitly address data transfers to international

228. Information Transparency & Personal Data Control Act, H.R. 1816, 117th Cong. § 2(1) (2021).

229. *Id.* § 2(6)(E).

230. *Id.* § 3(a)(1), (a)(4).

231. *Id.* § 2(6)(F).

232. *Id.* § 3(a)(6)(A)(i). There is an exemption for the audit requirements for businesses that collect or use sensitive personal information for fewer than 250,000 individuals per year. *Id.* § 3(a)(6)(C).

233. *Id.* § 7(9)(A).

234. *Id.*

235. *Id.* § 7(9)(B).

236. *Id.* § 3(a)(1)(A). A "controller" is a "person that, on its own or jointly with other entities, determines the purposes and means of processing sensitive personal information." *Id.* § 7(5).

237. *Id.* § 3(a)(1)(A).

238. *Id.*

corporate affiliates.[239] For non-sensitive personal information, however, the Information Transparency and Personal Data Control Act provides consumers the right to opt-out of collection and use.[240]

Another bill before the 117th Congress that provides strong consumer data privacy rights is the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act ("SAFE DATA Act").[241] The requirements of the SAFE DATA Act would apply to any "covered entity," which the Act defines as "any person that is subject to the Federal Trade Commission Act . . . ; collects, processes, or transfers covered data; and determines the purposes and means of such collection, processing, or transfer."[242] "Covered data" means any information "that identifies or is linked or reasonably linkable to an individual or a device that is linked or reasonably linkable to an individual."[243]

Like the GDPR and CCPA/CPRA, the SAFE DATA Act would provide consumers with affirmative data privacy rights: the rights to access, correction, deletion, and data portability;[244] opt-in consent for the processing or transfer of sensitive covered data;[245] and opt-out consent for non-sensitive covered data.[246] The Act would also restrict covered entities to the collection, processing, or transfer of covered data to what "is reasonably necessary, proportionate, and limited to provide or improve a product, service, or a communication about a product or service."[247] The Act would require "large data holders" to conduct ongoing privacy impact assessments,[248] as well as require covered entities to "establish, implement,

239. *Id.* § 7(11). A "third party" is defined as "an individual or entity that uses or receives sensitive personal information obtained by or on behalf of a controller." *Id.*

240. *Id.* § 3(a)(4)(A).

241. Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act, S. 2499, 117th Cong. (2021).

242. *Id.* § 2(7).

243. *Id.* § 2(6)(A).

244. *Id.* § 103(a)(1)(A)–(C). The requirement to provide consumers with the right to access, correction, deletion, and data portability would not apply to certain small businesses that do not meet minimum thresholds. *Id.* § 108(c).

245. *Id.* § 104(a). The bill broadly defines "sensitive covered data," which includes data such as government-issued identification numbers, health data, financial account numbers, biometric information, precise geolocation data, log-in credentials, and sexual orientation, among others. *Id.* § 2(17).

246. *Id.* § 104(d).

247. *Id.* § 105(a)(1). The data minimization requirements would not apply to certain small businesses that do not meet minimum thresholds. *Id.* § 108(c).

248. *Id.* § 107(a)–(b). A "large data holder" is a business that in one calendar year processes or transfers (1) the non-sensitive data of more than eight million individuals or (2)

and maintain reasonable administrative, technical, and physical data security policies and practices to protect against risks to the confidentiality, security, and integrity of covered data."[249] In addition, the SAFE DATA Act would require covered entities to designate a "data privacy officer" and a "data security officer" to monitor and ensure compliance with the Act.[250] While the Act would regulate the transfer of data to third parties, third parties would not include entities that receive covered data from entities "related to the covered entity by common ownership or corporate control" and that "share common branding with the covered entity."[251] Thus, the Act would not regulate transfers to foreign-based corporate affiliates.

A third notable data privacy bill before Congress is the Data Protection Act of 2021.[252] Unlike other privacy bills, the Data Protection Act of 2021 does not enumerate specific data privacy rights. Rather, like the CPRA, the Act would establish an independent agency—the "Data Protection Agency"[253]—whose purpose would be "to protect individuals' privacy, prevent and remediate privacy harms, prevent, remediate, and reduce discrimination on the basis of protected class through the processing of personal information . . . , and limit the collection, processing, and sharing of personal data."[254] The Data Protection Agency would be empowered to issue rules, orders, and guidance necessary to carry out the Act and enforce other federal privacy laws.[255] Although the Data Protection Act of 2021 does not enumerate specific data privacy rights, the Data Protection Agency would have authority to prescribe and enforce such rights to "protect[] individuals and groups of individuals from privacy harms."[256]

If Congress were to enact any of the abovementioned bills, U.S. consumers would enjoy data privacy rights resembling those under the GDPR and the CCPA/CPRA, which would be a significant step toward protecting data privacy in the United States. A shortcoming of these bills, however, is that they do not explicitly address the privacy- and national-security-related issues of cross-border data transfers.

---

the sensitive data of more than three-hundred thousand individuals. *Id.* § 2(12).

249. *Id.* § 203(a).
250. *Id.* § 301(a)–(b).
251. *Id.* § 2(20).
252. Data Protection Act of 2021, S. 2134, 117th Cong. (2021).
253. *Id.* § 3(a).
254. *Id.* § 9(a).
255. *Id.* § 10(b).
256. *Id.* § 9(c)(5).

The Adversarial Platform Prevention Act of 2021 ("APP Act"),[257] on the other hand, is specifically designed to prevent cross-border data flow from jeopardizing U.S. national security. The Act would require "high-risk foreign software, like Chinese-owned TikTok and WeChat," to comply with certain data privacy standards to legally operate in the United States.[258] Specifically, the APP Act would apply to "software marketplace operator[s]" and "owner[s] of covered foreign software."[259] "Software marketplace operators" are persons who, "for a commercial purpose, operate[] an online store or marketplace through which software is made available for download by consumers in the United States,"[260] and "covered foreign software" includes software "owned or directly or indirectly controlled" by a person that is organized, conducts its principal operations, or is headquartered in a "covered country."[261] A "covered country" means China, Russia, North Korea, Iran, Syria, Sudan, Venezuela, or Cuba, as well as any country that the U.S. Secretary of State concludes has supported international terrorism, or that by controlling "potentially dangerous software poses an undue or unnecessary risk to the national security of the United States or to the safety and security of United States persons."[262]

Although the APP Act does not provide broad data privacy rights like other bills before the 117th Congress, the Act would provide several data privacy protections for U.S. consumers. First, the Act would require software marketplace operators and owners of covered foreign software to provide consumers with a pre-download "warning" that lists the names of the software and software owner, as well as the country where the owner is organized, headquartered, or operates.[263] Second, the Act would require owners of covered foreign software to ensure that parent companies could not access U.S. consumer data through U.S.- or foreign-based subsidiaries.[264] Third, and most significantly, the APP Act would prevent software marketplace operators and owners of covered foreign software

257. Adversarial Platform Prevention Act of 2021, S. 47, 117th Cong. (2021).

258. Press Release, Marco Rubio, U.S. Senate, Rubio Reintroduces Legislation to Establish Standards and Restrictions for Chinese and Other High-Risk Foreign Apps (Jan. 26, 2021), https://www.rubio.senate.gov/public/index.cfm/2021/1/rubio-reintroduces-legislation-to-establish-standards-and-restrictions-for-chinese-and-other-high-risk-foreign-apps.

259. Adversarial Platform Prevention Act of 2021, S. 47 § 2(a)(1).

260. *Id.* § 2(i)(7).

261. *Id.* § 2(i)(4)(A)–(B).

262. *Id.* § 2(i)(3)(A).

263. *Id.* § 2(a)(1)–(2).

264. *Id.* § 2(b)(2)(C).

from using consumer data in a covered country, transferring consumer data to a covered country, or storing consumer data outside the United States.[265] In addition, the Act would require owners of covered foreign software to submit annual reports to the Federal Trade Commission and the U.S. Attorney General that explain the type of data the owner collects, describe their "data protection measure[s]," and list the number of data requests by foreign governments and government entities, as well as how such requests were handled.[266] If an owner of covered foreign software complies with a request from a government in covered foreign country, the owner is barred from collecting or storing data of any U.S. consumer through its covered foreign software.[267] Software marketplace operators and owners of covered foreign software are subject to criminal penalties of $50,000 for each knowing violation of the abovementioned data-protection measures.[268]

While the APP Act aggressively combats threats to data privacy and national security by regulating cross-border data flow, the Act has some glaring drawbacks. First, though other data privacy bills before Congress specifically define consumer data and distinguish between sensitive and non-sensitive data,[269] the APP Act does neither; the Act presumably applies to all consumer data, regardless of type and sensitivity level. Second, the Act would not only restrict data transfers to foreign-based entities—it specifies that owners of covered foreign software "may not share with, sell to, or otherwise disclose to *any other commercial entity* the consumer data of any person in the United States."[270] Rather than broadly prohibiting the of transfer of *any* consumer data to *any* commercial entity, calibrating transfer restrictions to the sensitivity level of consumer data would provide a more balanced approach without sacrificing privacy or security.

Striking a balance between the economic risks of data localization and the national security risks of foreign governments gaining access to U.S. personal data is a complex but necessary challenge for a federal data privacy law. Lawmakers should further debate and explore how to best regulate cross-border data flows. This Comment recommends that a U.S. federal data privacy law include the strong data privacy rights of bills like the SAFE DATA Act, as well as provisions regulating cross-border data

265. *Id.* § 2(b)(3)(A).
266. *Id.* § 2(b)(1)(A).
267. *Id.* § 2(b)(2)(A).
268. *Id.* § 2(e)(1).
269. *See supra* notes 233–35 and accompanying text (Information Transparency and Personal Data Control Act); *see also supra* notes 243–46 (SAFE DATA Act).
270. Adversarial Platform Prevention Act of 2021, S. 47 § 2(b)(3)(B) (emphasis added).

flow, including between U.S.-based subsidiaries and their international corporate affiliates. Furthermore, such a law should (1) establish an independent agency that regulates cross-border data transfers to entities or countries that do not afford adequate data protection and is empowered to enter into data-protection agreements with those countries; (2) calibrate transfer restrictions through risk-based assessments that consider the type, use, and sensitivity level of consumer data;[271] and (3) require companies to conduct regular assessments regarding companies' and receiving entities' data protection compliance in cross-border transfers. The U.S. government should further support these measures through the inclusion in trade negotiations of cross-border data protection standards that would loosen data localization policies while protecting data privacy and both countries' national security.

Conclusion

The TikTok and WeChat debacle has illustrated IEEPA's inability to combat threats that foreign mobile applications pose to U.S. national security and data privacy. Rather than one-off uses of IEEPA that target individual foreign mobile applications, the United States should adopt a comprehensive approach to protecting national security and privacy in the form of a federal consumer data privacy law. Privacy is an internationally recognized human right, and the U.N. human rights machinery has indicated that this right extends to data privacy.[272] Furthermore, under the UNGPs, the United States is required to pass legislation that protects internationally recognized human rights.[273] This legislation should provide the strong data privacy rights of laws such as the GDPR and the CCPA/CPRA, which would give consumers more control over their personal information. Several of the bills before the 117th Congress would provide for these rights. But to help prevent future TikTok and WeChat scenarios, a federal data privacy law should also regulate cross-border data

271. *See generally* Sacks, *supra* note 227 ("The mere fact that a Chinese company handles U.S. citizen data in and of itself may not necessarily warrant banning a transaction or blacklisting a specific company. The U.S. national security risks should be evaluated based on an investigation, with regular audits, to determine (a) what kind of U.S. citizen data is being accessed (for example, metadata, images, geographic data, critical infrastructure data), (b) how that data is being used and what data protection measures are in place to protect the rights and interests of U.S. consumers, and (c) with whom that data is being shared and through what mechanisms.").

272. G.A. Res. 68/167, *supra* note 132.

273. *See supra* notes 137–38 and accompanying text.

transfers based on the type and sensitivity level of consumer data. This is where the current bills fall short.

In light of U.S. fears that foreign governments can obtain U.S. citizens' personal information through foreign mobile applications, a federal consumer data privacy law must provide a nuanced approach to cross-border data transfers that balances national security interests with the harmful effects of data localization. Without such a federal law, the United States will continue "playing a game of whack-a-mole" against an increasing number of foreign technology companies.[274]

Robert L. Rembert

274. Samm Sacks, *Banning TikTok Is a Terrible Idea*, SUPCHINA (July 16, 2020), https://supchina.com/2020/07/16/banning-tiktok-is-a-terrible-idea/.