The National Security Internet

ANUPAM CHANDER*

In response to widespread foreign surveillance and growing geopolitical distrust, governments are erecting a national security internet. Pioneered by China, national firewalls have gone global. But where firewalls sought to keep information out, they now seek to keep data in. Governments keen to avoid their citizens' data from falling into foreign hands demand not only that personal data be stored on local servers, but also require that it be stored on local servers by local companies—what this Article calls "data localization squared." Enforcing this demand requires a new mechanism of transnational control: immunity from foreign jurisdiction. Artificial Intelligence (AI) systems, too, now need licenses for export. We are witnessing the creation of Digital Berlin Walls, complete with Checkpoint Charlies to permit border crossings.

The ascent of digital border controls in the name of national security treats a domain of speech and commerce according to the rules of war. This Article traces this turn through six case studies: TikTok, the United States "rip and replace" program, the Chinese "Delete America" program, Microsoft 365, connected cars, and AI models. The TikTok saga is but the visible edge of a broad reconfiguration of international economic relations largely occurring through obscure administrative processes. Existing scholarship has recognized various aspects of this national security turn; this Article weaves together regulatory moves from TikTok to cars, from the United States to China, to identify a paradigm shift in digital regulation.

The Article argues that the national security internet will come at a steep price, disrupting trade and investment, reducing competition, inviting retaliation, increasing government control over speech, and undermining efforts to stem climate change and promote development, while offering easily circumvented protection against foreign surveillance. The Article introduces a typology of corporate strategies to satisfy national security demands and assesses their limitations. The Article proposes

* Scott K. Ginsburg Professor of Law and Technology, Georgetown Law. I thank Anu Bradford, William Dodge, Todd Huntley, Paul Schwartz, and Tim Wu for invaluable insights, Donara Aghajani, C. Duruhan Aydinli, Chirag Chhabra, Jonas Cruz, Daniel Csigirinszkij, Eyrna Jones-Heisler, Kurtis Lee, Fatema Lunawadawala, Chao Li, Bo Peng, Virginia Polik, Daniel Powell, Hazel Song, Huihui Wang, Lale Yilaliding, and Haiqi Zou at Georgetown and Irene Kim at Harvard for excellent research assistance, Jasmine Donohue-Özyar and Marcus Helble at *The Georgetown Law Journal* for editorial assistance, and commentators at workshops at Columbia Law School, Georgetown University, and the London School of Economics for suggestions. Much of the research for this paper was conducted during a fellowship at the Institute for Rebooting Social Media at Harvard. The author led two amicus briefs on behalf of First Amendment and internet scholars in a challenge to the law requiring either a sale or a ban of TikTok. *See infra* note 212. All views are my own.

reforms that constrain foreign surveillance in order to protect both civil rights and national security.

TABLE OF CONTENTS

INTRODUCTION

The Great Firewall of China has gone global. But rather than seeking to staunch the flow of foreign information infiltrating into the domestic sphere, digital firewalls seek to prevent data from flowing out. Even China's own digital firewall has been reconceived for this purpose—from its origin as a "Golden Shield" against foreign influence in domestic information systems to its new role as a barrier to the gathering of data by foreign powers.[1] Before transferring data out of China, many companies now need to pass an explicit "data exit security assessment" seeking to ensure that transfer of information abroad does not pose security risks back home.[2]

But China is hardly alone. What is perhaps more surprising is that laws and regulations across the world increasingly require border checks for exiting data.[3]

---

1. *See* Yaqiu Wang, *In China, the 'Great Firewall' Is Changing a Generation*, POLITICO: MAGAZINE (Sep. 1, 2020, at 04:30 EDT), https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385 [https://perma.cc/RD6Z-8399] ("China's internet censorship system, colloquially known as the Great Firewall, has existed since 2000, when the Ministry of Public Security launched the Golden Shield Project, a giant mechanism of censorship and surveillance . . . .").

2. *See China: CAC Issues Data Export Security Assessment Measures*, DATAGUIDANCE (July 7, 2022), https://www.dataguidance.com/news/china-cac-issues-data-export-security-assessment [https://perma.cc/XD6F-GF8T]; Rogier Creemers, Samm Sacks, Graham Webster & Lorand Laskai, *Translation: Outbound Data Transfer Security Assessment Measures (Draft for Comment) – Oct. 2021*, STAN. UNIV.: DIGICHINA (Oct. 29, 2021), https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021 [https://perma.cc/2QS9-BQLF].

3. *See* Mark A. Lemley, *The Splinternet*, 70 DUKE L.J. 1397, 1404 (2021) (discussing a "Eurocentric bias against U.S. tech companies," and noting "a European court order blocking transfers of data to the United States because of concerns about U.S. surveillance").

The United States has brought a growing arsenal of international economic law tools—from international emergency economic powers,[4] to foreign investment reviews,[5] to export controls[6]—to scrutinize the outward flow of data on national security grounds.[7] Even privacy law is being yoked into service: the proposed bipartisan American Privacy Rights Act, while not blocking data flows to foreign countries, requires companies to disclose whether data is transferred to China.[8] The Biden Administration's Executive Order on Artificial Intelligence included an array of measures designed to prevent foreign adversary nations from accessing advanced AI services.[9] The United States has employed foreign investment reviews to unwind a Chinese acquisition of the dating app Grindr and to reject a Chinese acquisition of MoneyGram.[10] Most famously, in April 2024, the United States passed a law requiring the Chinese owners of TikTok to either sell the company or see TikTok banned from the United States by January 19, 2025.[11]

Over the last decade, many have observed the rise of "data localization"—the requirement that data be stored and processed within its country of origin.[12] But as the TikTok example demonstrates, localizing data on domestic servers (as TikTok offered through its Project Texas mitigation proposal)[13] is no longer enough. Now data must be put *on local servers controlled by local companies*, what we might call "data localization squared." This Article identifies the

4. *See* CHRISTOPHER A. CASEY & JENNIFER K. ELSEA, CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE 8–10 (2024).

5. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-107358, FOREIGN INVESTMENT IN THE U.S.: EFFORTS TO MITIGATE NATIONAL SECURITY RISKS CAN BE STRENGTHENED 4 (2024).

6. *See* Chad P. Bown, *Export Controls: America's Other National Security Threat*, 30 DUKE J. COMPAR. & INT'L L. 283, 287 (2020) (discussing how, "[a]lmost from inauguration day, the Trump administration tied together trade and national security in ways not seen in U.S. policy for decades").

7. Kristen E. Eichensehr & Cathy Hwang, *National Security Creep in Corporate Transactions*, 123 COLUM. L. REV. 549, 560 (2023).

8. *See* American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. § 104(b)(9) (2024) (requiring disclosure if covered data is made accessible to an adversary country such as China). An earlier bipartisan privacy bill also included a nearly identical provision. *See* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 202(b)(9) (2022).

9. Exec. Order No. 14110, 88 Fed. Reg. 75191, 75198 (Nov. 1, 2023) (*inter alia*, taking steps to require United States Infrastructure as a Service (IaaS) providers to identify and maintain records of foreign persons using their services for AI training). President Trump repealed this order on his first day in office. *See* Exec. Order No. 14148, 90 Fed. Reg. 8237, 8240 (Jan. 28, 2025).

10. Yuan Yang & James Fontanella-Khan, *Grindr Is Being Sold by Chinese Owner After U.S. Raises National Security Concerns*, L.A. TIMES (Mar. 6, 2020, at 11:43 PT), https://www.latimes.com/business/technology/story/2020-03-06/grindr-sold-by-chinese-owner-after-us-national-security-concerns [https://perma.cc/ECZ8-ML84]; Ana Swanson & Paul Mozur, *MoneyGram and Ant Financial Call Off Merger, Citing Regulatory Concerns*, N.Y. TIMES (Jan. 2, 2018), https://www.nytimes.com/2018/01/02/business/moneygram-ant-financial-china-cfius.html (stating that CFIUS blocked Ant Financial's purchase of MoneyGram).

11. Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, 138 Stat. 955 (2024); *see infra* notes 112–14 and accompanying text.

12. *See, e.g.*, Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2015) (defining "data localization," and describing data localization measures as "those that specifically encumber the transfer of data across national borders").

13. *See* ByteDance Ltd., TikTok Ltd. & TikTok Inc., Draft National Security Agreement §§ 11.5, 11.8–11.10 (Parties' Draft as of Aug. 23, 2022) [hereinafter Draft National Security Agreement].

emergence of a new legal doctrine—*immunity from foreign jurisdiction*—which requires that local providers of digital services not be subject to any foreign compulsion. This entails a more radical ripping apart of the internet than data localization alone. While this doctrine has been developed recently in the context of international data flows, it extends far beyond this domain—potentially to rules on ownership in broadcasting, telecommunications, and critical infrastructure. France's national cybersecurity agency, for example, requires "*immunité au droit extracommunautaire*"—immunity from non-EU law—as a condition for supplying cloud services for government agencies as well as operators of vital and essential services.[14] French Finance Minister Bruno Le Maire made the goal plain: "[A] 'trustworthy' cloud computing alternative can be developed within Europe . . . by guaranteeing the location of servers on French soil as well as European ownership of the companies that store and process the data."[15] Google and Microsoft could provide cloud services, he continued, but only as long as they license their technologies to French companies.[16] The key requirement: the data cannot become accessible to companies subject to U.S. jurisdiction.[17] Quite simply, foreign companies need not apply.

These extraordinary demands reflect growing anxieties about geopolitical conflicts and real concerns about excessive foreign surveillance.[18] These efforts began in earnest after the Snowden revelations of 2013, which exposed the extent of U.S. foreign surveillance operations,[19] but have increased with revelations suggesting Russian election-related hacking of U.S. politicians and possible Chinese

14. Dominique Luzeaux, Cloud *Souverain: Souveraineté et Résilience, ou Confiance?* [*Sovereign* Cloud*: Sovereignty and Resilience, or Trust?*], 855 REVUE DÉFENSE NATIONALE 14, 20 (2022) (paper by director of the French Defense Digital Agency, arguing for national self-reliance rather than dependence on trusted, often foreign, partners); *see* Agence Nationale de la Sécurité des Systèmes d'Information [ANSSI], *Prestataires de Services d'Informatique en Nuage (SecNumCloud) Référentiel d'Exigences* [*Cloud Computing Service Providers (SecNumCloud) Requirements Framework*], Version 3.2.a, art. 19.6 (Sep. 21, 2021), https://www2.itif.org/2021-secnumcloud-3.2.a-english-version.pdf [https://perma.cc/Y64P-REK4] (stating that "the service provider must be established within a member state of the European Union"), *translated in* Nigel Cory, *"Sovereignty Requirements" in French—and Potentially EU—Cybersecurity Regulations: The Latest Barrier to Data Flows, Digital Trade, and Digital Cooperation Among Likeminded Partners*, INFO. TECH. & INNOVATION FOUND. (Dec. 10, 2021), https://itif.org/publications/2021/12/10/sovereignty-requirements-france-and-potentially-eu-cybersecurity [https://perma.cc/F5R6-WRZP].

15. Mathieu Rosemain, *France Embraces Google, Microsoft in Quest to Safeguard Sensitive Data*, REUTERS (May 17, 2021, at 8:24 EDT), https://www.reuters.com/technology/france-embraces-google-microsoft-quest-safeguard-sensitive-data-2021-05-17.

16. *Id.*

17. *See id.*

18. *Cf.* Mark Jia, *American Law in the New Global Conflict*, 99 N.Y.U. L. REV. 636, 638–39 (2024) (describing how U.S. law is being rewritten to confront a rising China).

19. Laura K. Donohue, *High Technology, Consumer Privacy, and U.S. National Security*, 4 AM. U. BUS. L. REV. 11, 12, 24–25 (2014); *see also* Glen Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013, at 15:23 EDT), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/9XDM-US8E] (discussing the content of documents revealing NSA surveillance practices provided to the media by Edward Snowden).

hacking of the U.S. Office of Personnel Management.[20] Governments are alarmed that granting companies subject to foreign jurisdiction access to their data poses an existential threat: namely, a nation of people subject to blackmail by a hostile foreign power.[21] Rather than the foundation for global speech and economic prosperity,[22] cross-border data flows are now seen as a national security threat.[23] This concern echoes through the halls of power from Beijing to Berlin, and from New Delhi to Washington, D.C.[24] The idea of an open and free global internet has gradually been replaced by a "splinternet," that is, the "drawing [of] national boundaries around the internet."[25] The "Pax Americana" of a global internet of free flows is being replaced by a growing reality of national security border controls, embraced by the United States itself.[26]

The emerging digital border controls reflect an about-face in the history of the internet. The internet famously began as a military project to ensure resilient communications in the event of war.[27] Designing a communications network to be "survivable . . . even in the thermonuclear era" meant avoiding "any central—and therefore vulnerable—control point."[28] Where national security then meant a decentralized architecture that resisted border controls, national security now seems to require border checks for data.

This Article argues that the national digital firewalls prove easy to evade while threatening the global speech and exchange promised by the internet, and proposes alternatives to address the very real concerns of foreign government surveillance animating the emerging national security internet. The "National Security Internet" described here reflects the extension of the aggrandizement of

---

20. *See, e.g.*, Julian E. Barnes & Edward Wong, *In Risky Hunt for Secrets, U.S. and China Expand Global Spy Operations*, N.Y. TIMES (Sep. 17, 2023), https://www.nytimes.com/2023/09/17/us/politics/us-china-global-spy-operations.html; David E. Sanger & Catie Edmondson, *Russia Targeted Election Systems in All 50 States, Report Finds*, N.Y. TIMES (July 25, 2019), https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html; Mike Levine, *22 Million Affected by OPM Hack, Officials Say*, ABC NEWS (July 9, 2015, at 15:17 ET), https://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731 [https://perma.cc/K9XZ-82MN]. Notably, in neither of these cases were foreign software services a key vector for the infiltration.

21. *See, e.g.*, Yang & Fontanella-Khan, *supra* note 10 (explaining that CFIUS had forced the Chinese owner of Grindr to sell the app because "CFIUS had feared that the Chinese government could use personal data given to the app by its 3.3 million users to blackmail U.S. citizens").

22. *See* Anupam Chander, *Googling Freedom*, 99 CALIF. L. REV. 1, 11 (2011); Anupam Chander, *Jasmine Revolutions*, 97 CORN. L. REV. 1505, 1513 (2012); Jennifer Daskal, *Speech Across Borders*, 105 VA. L. REV. 1605, 1613 (2019).

23. *See* Albert Gidari, *The Cross-Border Data Fix: It's Not So Simple*, STAN. UNIV.: CTR. FOR INTERNET & SOC'Y: BLOG (June 16, 2017, at 15:03 ET), https://cyberlaw.stanford.edu/blog/2017/06/cross-border-data-fix-its-not-so-simple [https://perma.cc/7T8Q-ZUHS].

24. *See* ANUPAM CHANDER, THE ELECTRONIC SILK ROAD: HOW THE WEB BINDS THE WORLD IN COMMERCE 50, 77–78, 169–70 (2013).

25. Lemley, *supra* note 3, at 1399.

26. *See* Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1684, 1736 (2018).

27. John Naughton, *The Evolution of the Internet: From Military Experiment to General Purpose Technology*, 1 J. CYBER POL'Y 5, 7 (2016).

28. PAUL BARAN, RAND CORP., ON DISTRIBUTED COMMUNICATIONS: I. INTRODUCTION TO DISTRIBUTED COMMUNICATIONS NETWORKS, at v, 16 (1964).

the Executive Branch over foreign affairs that has characterized decades of presidential actions.[29] Harold Koh argues that this unilateralist executive control stands contrary to the "National Security Constitution," the "substructure of U.S. constitutional norms that protects the operation of checks and balances in national security policy."[30] Koh argues that the legislative and judicial branches play a critical role in foreign affairs, writing that "the power to conduct American foreign policy is not exclusively presidential, but is a power shared among the president, the Congress, and the courts."[31] Earlier debates about embargoes, war powers, and steel seizures have now been joined by debates over executive powers over foreign internet speech platforms.

The issue of border controls for data is also critical for the mainstays of international economic law: trade, investment, and finance. First, consider international trade, which is at risk as data must undergo a border security check.[32] Data insecurity threatens to tear the internet apart into separate trading zones.[33] In a recent book, Anu Bradford argues that the United States, the EU, and China are promulgating three digital empires, based on incompatible visions of the internet.[34] This Article argues that even while the three governments may be seeking to export their visions, they are simultaneously building digital firewalls between their own empires, threatening both trade and information flows. In a sense, the Digital Walls described in this Article are an effort to keep foreign digital empires out. Perhaps most dramatically, first in 2020, and again in 2024, the United States government ordered the divestiture of TikTok by its Chinese owners, arguing that a major social media enterprise operating in the United States could not be owned by a company from China for fear that the data might flow with ownership.[35] But

---

29. *See, e.g.*, Jonathan Masters, *U.S. Foreign Policy Powers: Congress and the President*, COUNCIL ON FOREIGN RELS. (Mar. 2, 2017, at 14:28 EST), https://www.cfr.org/backgrounder/us-foreign-policy-powers-congress-and-president [https://perma.cc/34DH-UW6T] ("[P]residents have accumulated power at the expense of Congress in recent years as part of a pattern in which, during times of war or national emergency, the executive branch tends to eclipse the legislature.").

30. HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION IN THE TWENTY-FIRST CENTURY 1 (2024).

31. *Id.*

32. *See* Henry Gao, *Data Sovereignty and Trade Agreements: Three Digital Kingdoms*, *in* DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE 213, 218–19 (Anupam Chander & Haochen Sun eds., 2023).

33. *See* Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 J. INT'L ECON. L. 245, 268–70 (2018); Gao, *supra* note 32, at 213, 236–38.

34. *See generally* ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY (2023).

35. Exec. Order No. 13942, 85 Fed. Reg. 48637 (Aug. 11, 2020) (IEEPA executive order banning transactions with TikTok); *Presidential Order Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51297 (Aug. 19, 2020) (CFIUS-based executive order requiring divestment). The Biden Administration withdrew the TikTok ban order, but put the CFIUS divestiture order on hold, continuing its security review. *See* TikTok Inc. v. Garland, 122 F.4th 930, 943 (D.C. Cir. 2024). Instead, the company spent the last few years under the cloud of the investment order, seeking to negotiate a security arrangement that satisfies the U.S. government without divestiture. *See infra* notes 356–68 and accompanying text.

even as the United States kicks out the Chinese owners of TikTok, China is seeking to "delete America" from the government's technology stack.[36] Because modern goods trade increasingly relies on cross-border data flows, the national security turn in internet regulation affects both digital services and modern goods, and undermines global goals to promote economic development and slow climate change. Concerns about cross-border data flows threaten the sale of Chinese electric cars,[37] drones,[38] and even fast fashion and household goods.[39]

Second, international investments have been blocked because of the risk that data about a nation's citizens might fall into the wrong foreign hands.[40] After a U.S. divestiture order for a Chinese company's acquisition of a cloud-based hotel management software company, other companies worried about all Chinese acquisitions because "almost every American company collects data on its users."[41]

Third, even international financial markets stand at risk. Chinese companies offering registered securities in the United States were under threat of delisting, caught between U.S. securities regulators' demands for audit data for such companies, and Chinese government concerns about U.S. government access to that data.[42] In 2020, the U.S. Congress passed the Holding Foreign Companies Accountable Act, which heightened disclosure requirements for Chinese companies listing on U.S. exchanges and added penalties for noncompliance with U.S.

---

36. Liza Lin, *China Intensifies Push to 'Delete America' from Its Technology*, WALL ST. J. (Mar. 7, 2024, at 00:01 ET), https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f (reporting on "Document 79," which "requires state-owned companies in finance, energy and other sectors to replace foreign software in their IT systems by 2027").

37. *See infra* notes 269–83 and accompanying text (describing the connected vehicles rules). For its part, China requires data localization for Tesla's operations in China. Trefor Moss, *Tesla to Store China Data Locally in New Data Center*, WALL. ST. J. (May 26, 2021, at 03:43 ET), https://www.wsj.com/business/autos/tesla-to-store-china-data-locally-in-new-data-center-11622015001. China had already banned Tesla cars from certain government buildings for fear that they may transmit secrets to foreign powers. *See* James Andrew Lewis, *Connected Cars and Spying*, CTR. FOR STRATEGIC & INT'L STUD. (Oct. 1, 2024), https://www.csis.org/analysis/connected-cars-and-spying [https://perma.cc/A8DX-BYS7]; *Tesla Cars Barred from Some China Government Compounds - Sources*, REUTERS (May 21, 2021, at 00:37 ET), https://www.reuters.com/world/china/tesla-cars-barred-some-china-government-compounds-sources-2021-05-21. On U.S. fears about Chinese drones, see *infra* 232–239 and accompanying text.

38. *See infra* notes 230–40 and accompanying text (describing rules against certain Chinese drones).

39. NICHOLAS KAUFMAN, U.S.-CHINA ECON. & SEC. REV. COMM'N, SHEIN, TEMU, AND CHINESE E-COMMERCE: DATA RISKS, SOURCING VIOLATIONS, AND TRADE LOOPHOLES 2–3, 5–6 (Apr. 14, 2023) (raising data concerns about Shein and Temu).

40. In 2019, CFIUS ordered the divestiture of the dating app Grindr, as well as online health service PatientsLikeMe, both of which had been acquired by Chinese entities. *See* Yang & Fontanella-Khan, *supra* note 10; Christina Farr & Ari Levy, *The Trump Administration Is Forcing This Health Start-Up That Took Chinese Money into a Fire Sale*, CNBC (Apr. 4, 2019, at 12:57 ET), https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html [https://perma.cc/DN8M-RGMY].

41. Ana Swanson, *Trump Administration Blocks Chinese Acquisition of Hotel Software Company*, N.Y. TIMES (Mar. 6, 2020), https://www.nytimes.com/2020/03/06/business/economy/trump-administration-blocks-chinese-acquisition-cfius.html.

42. Lulu Yilun Chen & John Cheng, *China State-Owned Giants to Delist from US Amid Audit Spat*, BLOOMBERG (Aug. 12, 2022, at 10:15 ET), https://www.bloomberg.com/news/articles/2022-08-12/china-state-owned-giants-plan-to-delist-from-us-amid-audit-spat.

securities disclosure requirements.[43] The U.S. Securities and Exchange Commission requires that the U.S. Public Company Accounting Oversight Board have access to underlying audit records for all companies that are publicly listed in the United States.[44] The Chinese government was concerned that this would undermine China's national security; as one expert observes, "These state-owned enterprises are in strategic sectors and deemed to have access to information and data that the Chinese government may be hesitant to give access to foreign regulators."[45] Accordingly, some of the largest Chinese companies announced plans to delist from the New York exchanges.[46] Didi was forced to delist from the NY Stock Exchange "due to [Chinese government] worries about leakage of sensitive data."[47] The government standoff was alleviated when China permitted U.S. regulators to access audit data,[48] but the pause may only be temporary.[49] Fashion giant Shein's planned 2024 IPO in New York was foiled by cybersecurity concerns—both in the United States and China.[50] Facing both backlash from U.S. lawmakers and Chinese government scrutiny about U.S. government access to Chinese personal data, Shein scrapped its U.S. IPO, leading it to turn to Hong Kong for a possible listing.[51]

---

43. Holding Foreign Companies Accountable Act, Pub. L. No. 116-222, § 3, 134 Stat. 1063, 1064–66 (2020) (increasing auditing frequency from every three years required for all companies to every two years for Chinese companies and requiring disclosure of connections to Chinese government and the Chinese Communist Party).

44. *See Auditing the Auditors: Creating the Public Company Accounting Oversight Board*, SEC HIST. SOC'Y, https://www.sechistorical.org/museum/galleries/pcaob [https://perma.cc/C6YN-KAV6] (last visited Dec. 29, 2025).

45. Chen & Cheng, *supra* note 42.

46. Five major Chinese companies, China Life Insurance Company, PetroChina Company Limited, China Petroleum & Chemical Corporation, Aluminum Corporation of China Limited, and Sinopec Shanghai Petrochemical Company Limited, announced plans to delist from the New York Stock Exchange. *Id.*

47. Julie Zhu, Kane Wu & Brenda Goh, *Beijing Presses Didi to Delist from U.S. Over Data Security Fears*, REUTERS (Nov. 26, 2021, at 10:39 ET), https://www.reuters.com/world/china/china-asks-didi-delist-us-security-fears-bloomberg-news-2021-11-26 [https://perma.cc/UHZ4-A7VG]; *see also* Shiyin Chen & Coco Liu, *Didi's Move From NYSE to Hong Kong — What to Know*, BLOOMBERG (May 23, 2022, at 13:56 ET), https://www.bloomberg.com/news/articles/2021-12-03/everything-we-know-about-didi-s-plan-to-delist-from-the-nyse (noting the Chinese government's "concerns about leakage of sensitive data").

48. Laura He, *Delisting Risks for China Tech Stocks Averted as US Gets 'Historic' Access to Audit Data*, CNN: BUS. (Dec. 16, 2022, at 01:09 EST), https://www.cnn.com/2022/12/16/business/china-stock-us-delisting-averted-audit-access-intl-hnk/index.html [https://perma.cc/TEW8-LUN4].

49. Jesse M. Fried & Tamar Groswald Ozery, *The Holding Foreign Companies Accountable (HFCA) Act: A Critique* 16–17 (Eur. Corp. Governance Inst., Working Paper No. 721/2023), http://ssrn.com/abstract_id=4505890 [https://perma.cc/PK4H-JYCP] (arguing that Chinese authorities might again refuse access to such records in the future).

50. Liza Lin & Raffaele Huang, *Fashion Giant Faces New IPO Hitch: China's Cybersecurity Police*, WALL ST. J. (Jan. 16, 2024, at 22:50 ET), https://www.wsj.com/world/china/fashion-giant-faces-new-ipo-hitch-chinas-cybersecurity-police-70c57561.

51. *See id.*; James Fontanella-Khan, Eleanor Olcott, Mercedes Ruehl, Arash Massoudi & Ivan Levingston, *Shein Switches Focus to London After New York IPO Stalls*, FIN. TIMES (May 16, 2024), https://www.ft.com/content/300d0a15-2e4b-44a0-b3c8-5078a9e30ae2. Shein's alternative plan for a London Stock Exchange listing failed to receive approval from the China Securities Regulatory Commission, leading Shein to retreat to Hong Kong. Julie Zhu, Hadeel Al Sayegh & Helen Reid,

This Article builds on existing literature. Mark Lemley worries about the harms of the "Splinternet."[52] Kristen Eichensehr and Cathy Hwang describe the security creep in U.S. foreign investment law.[53] Kathleen Claussen discusses how U.S. national security law permits the erection of barriers that seemingly undermine trade, and argues that national security statutory authorities have become unmoored from their original purposes.[54] J. Benton Heath highlights the security creep in international trade law.[55] Mona Pinchis-Paulsen sheds light on the interpretation of the national security exception in modern trade law through a study of its historical origins.[56] Neha Mishra argues that cybersecurity measures that governments are now taking, which disadvantage foreign suppliers, may not be able to successfully avail themselves of the national security exceptions in trade law.[57] Uyên P. Lê and I have cautioned against threats to both civil and economic liberties from emerging practices of data localization.[58] Paul Schwartz has evaluated the panoply of U.S. legal authorities that permit parties to seek data held abroad.[59] Paul Schwartz and I have observed the rising conflict between data privacy and trade,[60] and the national security turn in U.S. data policy.[61] Ganesh Sitaraman defends the national security turn in regulating foreign platforms based on what he describes as a long history of similar restrictions.[62] Henry Farrell and Abe Newman incisively show the weaponization of international economic tools by the United States.[63] Theodore Christakis has labeled the logic leading to the shutting out of foreign digital services the "zero-risk fallacy" because it relies on two mistaken propositions: "(1) the misconception that data transfers, to be permissible, must essentially be risk-free, i.e., 'zero risk'; and (2) that data localization

Exclusive: Shein Working Towards Hong Kong Listing After London IPO Stalls, Say Sources, REUTERS (May 28, 2025, at 05:29 ET), https://www.reuters.com/business/finance/shein-working-towards-hong-kong-listing-after-london-ipo-stalls-say-sources-2025-05-28.

52. *See* Lemley, *supra* note 3, at 1399 ("The balkanization of the internet is a bad thing, and we should stop it if we can.").

53. *See generally* Eichensehr & Hwang, *supra* note 7.

54. *See* Kathleen Claussen, *Trade's Security Exceptionalism*, 72 STAN. L. REV. 1097, 1142–49 (2020).

55. *See generally* J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L.J. 1020 (2020).

56. *See generally* Mona Pinchis-Paulsen, *Trade Multilateralism and U.S. National Security: The Making of the GATT Security Exceptions*, 41 MICH. J. INT'L L. 109 (2020).

57. *See* Neha Mishra, *The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance*, 54 J. WORLD TRADE 567, 569 (2020).

58. *See generally* Chander & Lê, *supra* note 12.

59. *See* Schwartz, *supra* note 26, at 1708.

60. *See generally* Anupam Chander & Paul Schwartz, *Privacy and/or Trade*, 90 U. CHI. L. REV. 49 (2023).

61. *See* Anupam Chander & Paul Schwartz, *The President's Authority over Cross-Border Data Flows*, 172 U. PA. L. REV. 1989, 2047 (2024).

62. *See generally* Ganesh Sitaraman, *The Regulation of Foreign Platforms*, 74 STAN. L. REV. 1073 (2022).

63. *See* HENRY FARRELL & ABRAHAM NEWMAN, UNDERGROUND EMPIRE: HOW AMERICA WEAPONIZED THE WORLD ECONOMY 3 (2023).

efforts resolve the risk of foreign government access to data."[64] Taken together, these scholars warn about (and in some cases, defend) the securitization of wide domains of international economic law. This Article extends this work, identifying and appraising the securitization of internet data flows—the building block of the digital economy. If "[s]oftware is eating the world,"[65] national security is now eating software.[66]

The argument unfolds as follows. Part I identifies the turn towards restrictions against outward-bound data flows in the three largest economies in the world—the United States, China, and the European Union. Part II reviews flashpoints demonstrating this national security turn in internet regulation, going from TikTok to Microsoft 365 to cars and cranes. Part III argues that broad national security firewalls are easy to evade, undermine competition, prove expensive, harm trade, are intrusive, and, worst of all, increase the risk of authoritarian control. Just as the USA PATRIOT Act expanded U.S. government powers in the name of national security with insufficient protections for civil liberties,[67] we should

64. THEODORE CHRISTAKIS, CTR. FOR INFO. POL'Y LEADERSHIP & CROSS-BORDER DATA F., THE "ZERO RISK" FALLACY: INTERNATIONAL DATA TRANSFERS, FOREIGN GOVERNMENTS' ACCESS TO DATA AND THE NEED FOR A RISK-BASED APPROACH 3 (2024).

65. Marc Andreessen, *Why Software Is Eating the World*, ANDREESEN HOROWITZ (Aug. 20, 2011), https://a16z.com/2011/08/20/why-software-is-eating-the-world [https://perma.cc/3GNA-XXQU].

66. Digital border walls can be erected for other purposes as well. For example, the U.S. International Trade Commission has sought to regulate data flows into the United States to prevent alleged patent infringement. *See* Sapna Kumar, *Regulating Digital Trade*, 67 FLA. L. REV. 1909, 1924–25 (2015) (criticizing International Trade Commission's assertion of control over cross-border information flows as part of its efforts to protect against intellectual property infringement).

67. *See, e.g.*, DAVID COLE & JAMES X. DEMPSEY, TERRORISM AND THE CONSTITUTION: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY 195–218 (3d. ed. 2006) (discussing how the USA PATRIOT Act "cast a cloak of secrecy over the exercise of government power . . . [and] violated core constitutional principles"); Lisa Finnegan Abdolian & Harold Takooshian, *The USA PATRIOT Act: Civil Liberties, the Media, and Public Opinion*, 30 FORDHAM URB. L.J. 1429, 1434 (2003) (discussing how "[v]ery few news reports discussed the dangers involved in pushing aside civil liberties during a national crisis" and how "most stories about the country's response were positive"); Jacob R. Lilly, Note, *National Security at What Price: A Look into Civil Liberty Concerns in the Information Age Under the USA PATRIOT Act of 2001 and a Proposed Constitutional Test for Future Legislation*, 12 CORN. J.L. & PUB. POL'Y 447, 448 (2003) (arguing that the "egregious civil liberty violations in [the anti-terrorism efforts of the 1990s and 2000s] prove the inability of previous constitutional tests to curb those violations," and advocating for "a more effective test that still allows the government the necessary tools to protect the United States from external enemies"); Caspar Bowden, Pol'y Dep't: Citizens Rts. & Const. Affs., *The US Surveillance Programmes and their Impact on EU Citizens' Fundamental Rights*, EUR. PARL. DOC. (PE 474.405) 9 (2013) ("[T]he scope of surveillance conducted under a change in the FISA law in 2008 extended its scope beyond interception of communications to include any data in public cloud computing as well [which] has very strong implications for the EU's continued sovereignty over data and the protection of its citizens' rights."); James M. Lutz & Georgia Wralstad Ulmschneider, *Civil Liberties, National Security and U.S. Courts in Times of Terrorism*, 13 PERSP. ON TERRORISM 43, 43 (2019) ("Civil liberties in democratic countries have been threatened by counterterrorism measures that sacrifice liberty for security [and] [t]he United States has been no exception."); Christopher P. Raab, *Fighting Terrorism in an Electronic Age: Does the Patriot Act Unduly Compromise our Civil Liberties?*, 4 DUKE L. & TECH. REV. 1, ¶ 4 (2006) (finding that Sections 210 and 505 of the USA PATRIOT Act "infringe upon citizens' civil liberties to a degree incommensurate with their value for fighting terrorism"). *But see* Adrian Vermeule, *Self-Defeating Proposals: Ackerman on Emergency Powers*, 75 FORDHAM L. REV. 631, 633, 635 (2006) (explaining

worry about the rise of national security controls over the internet. Such expanded national security controls often offer what Shirin Sinnar has called "rule of law tropes," measures that hide excessive executive powers behind a regulatory façade.[68] Part IV builds on Kristen Eichensehr's concept of "Digital Switzerlands" to show how companies are attempting to navigate global geopolitics.[69] Part V proposes restraints on foreign surveillance to address the core concerns animating the national security internet.

I. THE RISE OF DIGITAL WALLS

The Great Firewall of China is now met by the Digital Walls of the United States and Europe. The world's largest economies are erecting barriers to each other's firms, fearing that those firms might be compelled to serve as spies for their home countries. This Part shows the development of digital firewalls in the United States, China, and the European Union, jurisdictions chosen because they represent the world's three largest economies.[70] While our focus is on these three jurisdictions, the issue is far broader.[71]

---

that Ackerman's premise that "[p]anicky lawmakers enact bad legislation, meaning unnecessarily oppressive and liberty-restricting legislation, such as the USA PATRIOT Act" should be tempered with recognition that "in the United States the national legislature and the judiciary retain substantial powers; America's federal system would complicate any attempt by a President to draw together all the strings of power; media that are traditionally skeptical of executive power would need to be shut down; a robust civil society—churches, clubs, universities, civic organizations—would need to squelched"); PRIV. & C. L. OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 1 (2014) (noting that § 215 of the USA PATRIOT Act authorized bulk telephone metadata collection and that § 702 of the FISA Amendments Act authorized content collection of non-U.S. persons' communications); OFF. OF THE INSPECTOR GEN., DOJ, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS, at viii (2016) (providing a summary of "the effectiveness and use, including any improper or illegal use, of national security letters issued by the Department of Justice"); Robert J. Graves & Indranil Ganguli, *Extraterritorial Application of the USA PATRIOT Act and Related Regimes: Issues for European Banks Operating in the United States*, 2 PRIV. & DATA SEC. L.J. 967, 967–68 (2007) ("[The USA PATRIOT Act's] most fundamental aim is to increase the amount and quality of information available to U.S. authorities responsible for preventing terrorism and other criminal activities [through] expand[ing] the allowable methods of information gathering, improv[ing] information sharing among government agencies, and increase[ing] funding for certain intelligence projects.").

68. Shirin Sinnar, *Rule of Law Tropes in National Security*, 129 HARV. L. REV. 1566, 1568–70 (2016).

69. *See* Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. 665, 696 (2019).

70. *See* EUROSTAT, CHINA, US AND EU ARE THE LARGEST ECONOMIES IN THE WORLD (2020), https://ec.europa.eu/eurostat/documents/portlet_file_entry/2995521/2-19052020-BP-EN.pdf/bb14f7f9-fc26-8aa1-60d4-7c2b509dda8e [https://perma.cc/SV4E-WTM7].

71. For example, India banned Chinese apps for excessive data collection about Indian citizens as an explicit "digital strike" in response to the literal hurling of stones between Chinese and Indian troops in the Himalayas. *'Banning Chinese Apps a Digital Strike': Union Minister Ravi Shankar Prasad*, HINDUSTAN TIMES (July 2, 2020, at 13:16 IST), https://www.hindustantimes.com/india-news/banning-chinese-apps-a-digital-strike-union-minister-ravi-shankar-prasad/story-XQQbTVt4bauqeBHfXC75iM.html [https://perma.cc/2SHQ-9WCA]. The Japanese messaging company Line faced criticism when it was revealed that engineers in China had access to data of Line users. Kenji Minemura & Toshiya Obu, *Personal Data of Millions of Line Users Accessed by Affiliate in China*, ASAHI SHIMBUN (Mar. 17, 2021, at 19:38 JST), https://www.asahi.com/ajw/articles/14276271 [https://perma.cc/3G6V-MKDL]. Line had contracted with another Japanese company to review notifications of

These regulatory moves are occurring within a geopolitical context. This is "lawfare" in action, war by other means. A low-level "Tech Cold War" seems afoot, with countries building defenses against each other.[72] The United States initially proposed an Alliance for the Future of the Internet, which critics saw as an effort to cleave the internet into two—one free, and the other unfree.[73] Some saw in the proposal an effort to create a "no-China club" internet.[74] Facing pushback from its international partners, the United States ultimately opted for a broader Declaration for the Future of the Internet that "reaffirms and recommits its partners to a single global Internet."[75]

This Part begins by showing the growing arsenal of legal tools that the United States is assembling to stop data flows across the border in the interest of national security. It then uncovers the evolution of China's Great Firewall, from promoting censorship to protecting against foreign surveillance. A third section reveals that the European Union, too, has implemented protections against foreign surveillance, but it has done so through data protection law, not national security law. Emerging from this discussion is a unifying doctrine that can be found in each of the three jurisdictions—the doctrine of immunity from foreign jurisdiction—which is defined and analyzed in the final section.

A. THE UNITED STATES

In 2018, Google's former CEO, Eric Schmidt, predicted the fragmenting of the internet into two zones—one led by the United States, and the other by China.[76] *The New York Times* went further, arguing the internet might balkanize into three

---

inappropriate posts, and that company had subcontracted with a Chinese company to review the posts, leading to the risk of inappropriate access. *Id.* Line responded by cutting off Chinese engineers' access to personal data, and also by promising to "rehome" personal data held in Korea. Laura Dobberstein, *LINE Stops Data Flowing to China After Japanese Officials Ditch App Over Privacy Concerns*, THE REGISTER (Mar. 24, 2021, at 03:31 UTC), https://www.theregister.com/2021/03/24/line_blocks_china_server_access [https://perma.cc/CE65-24FM]. Japan has also begun to designate cloud services as a national security concern, hoping to "cultivate domestic providers." Kosuke Takeuchi, *Japan to Label Cloud Services as Critical for Economic Security*, NIKKEI: ASIA (May 7, 2022, at 03:25 JST), https://asia.nikkei.com/Business/Technology/Japan-to-label-cloud-services-as-critical-for-economic-security [https://perma.cc/QZN6-MMKH]. Brazil's Supreme Court has upheld the power to compel companies to turn over data held abroad. SHANZAY PERVAIZ & ALEX JOEL, CTR. FOR INFO. POL'Y LEADERSHIP, DATA LOCALIZATION AND GOVERNMENT ACCESS TO DATA STORED ABROAD: DISCUSSION PAPER 2, at 5 (2023).

72. *See* Caitlin Lee, *Winning the Tech Cold War*, RAND (Aug. 17, 2023), https://www.rand.org/pubs/commentary/2023/08/winning-the-tech-cold-war.html [https://perma.cc/6W4M-R6DF].

73. *See* Jessica Brandt, *How Biden Can Make His Internet Freedom Agenda a Success*, BROOKINGS (Dec. 8, 2021), https://www.brookings.edu/articles/how-biden-can-make-his-internet-freedom-agenda-a-success [https://perma.cc/X3PE-KRRW].

74. CHARLES MOK, FRIEDRICH NAUMANN FOUND. FOR FREEDOM, THE EVERYTHING EVERYWHERE CENSORSHIP OF CHINA 46 (2023).

75. *Declaration for the Future of the Internet*, U.S. DEP'T STATE: BUREAU OF CYBERSPACE & DIGIT. POL'Y, https://www.state.gov/declaration-for-the-future-of-the-internet [https://perma.cc/GA3Q-A5P4] (last visited Dec. 29, 2025).

76. Lora Kolodny, *Former Google CEO Predicts the Internet Will Split in Two — and One Part Will Be Led by China*, CNBC (Sep. 21, 2018, at 15:41 EDT), http://cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html [https://perma.cc/A2FY-ZQN6] ("[T]he most likely scenario now is . . . a bifurcation into a Chinese-led internet and a non-Chinese internet led by America.").

zones—the United States, Chinese, and European internets.[77] One author, writing for the Council on Foreign Relations, encouraged the United States to "weaponize its digital trade," creating a digital trade zone that would exclude Chinese software and hardware through a "democratic digital supply chain."[78] That author would become the architect of the Biden Administration's national cyber strategy at the Office of the National Cyber Director.[79]

The United States has deployed a variety of legal tools to assert authority over cross-border data flows in the name of national security. The principal legal tool invoked for such purposes is the International Emergency Economic Powers Act of 1977 (IEEPA), which provides the President and the Executive Branch with broad powers to respond to international economic emergencies.[80]

The President's power to staunch cross-border data flows under IEEPA is complicated by a significant exception to this statute. In 1988, Congress amended IEEPA to explicitly exclude the ability to regulate cross-border transfer of "informational materials" from the authority granted to the President under the statute.[81] What would come to be known as the Berman Amendment, after its sponsor, Representative Howard Berman, excluded regulation of "the importation from any country, or the exportation to any country, whether commercial or otherwise, of publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, or other informational materials."[82] Thus, Congress denied the President the power to block the flows of informational materials, specifically mentioning the variety of forms that such materials might come in at that time. Congress acted "[o]ut of concern that [the Office of Foreign Assets Control's] administration of the trade sanctions programs was interfering with the free exchange of ideas and information."[83]

---

77. *There May Soon Be Three Internets. America's Won't Necessarily Be the Best.*, N.Y. TIMES (Oct. 15, 2018), http://nytimes.com/2018/10/15/opinion/internet-google-china-balkanization.html.

78. ROBERT K. KNAKE, COUNCIL ON FOREIGN RELS., WEAPONIZING DIGITAL TRADE: CREATING A DIGITAL TRADE ZONE TO PROMOTE ONLINE FREEDOM AND CYBERSECURITY, at v, 2 (2020).

79. Suzanne Smalley, *White House Cyber Official Rob Knake to Depart*, THE RECORD (June 14, 2023), https://therecord.media/white-house-oncd-cyber-official-rob-knake-to-depart-national-cyber-strategy [https://perma.cc/R4BU-4SJ3].

80. 50 U.S.C. § 1701(a) ("[The President is entitled] to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat."); Bruce Ackerman, *The Emergency Constitution*, 113 YALE L.J. 1029, 1079 n.113 (2004); Andrew Boyle, *An Emergency or Business as Usual? Huawei and Trump's Emergency Powers*, JUST SEC. (May 24, 2019), https://www.justsecurity.org/64252/an-emergency-or-business-as-usual-huawei-and-trumps-emergency-powers [https://perma.cc/GZB7-XAS8].

81. 50 U.S.C. § 1702(b)(3). The original version of the statute, as enacted in 1977, protected the rights of U.S. persons to exchange "any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value" across borders. International Emergency Economic Powers Act, Pub. L. No. 95-223, § 203(b)(1), 91 Stat. 1626, 1627 (1977) (codified as amended at 50 U.S.C. § 1702(b)). This remains in the statute today. *See* 50 U.S.C. § 1702(b)(1).

82. Limitation on Exercise of Emergency Authorities, Pub. L. No. 100-418, sec. 2502(b)(1)(C), § 203(b), 102 Stat 1107, 1371 (1988).

83. Tracy J. Chin, Note, *An Unfree Trade in Ideas: How OFAC's Regulations Restrain First Amendment Rights*, 83 N.Y.U. L. REV. 1883, 1891 (2008). Senator Charles Mathias, Jr. of Maryland, the sponsor of a Senate bill that also sought to add an informational materials exception to IEEPA, made

Congress trusted the American people to make up their own minds, even after exposure to foreign propaganda.[84]

The informational materials exception not only let information flow into the country; it sought to ensure that information could flow out. By its own terms, the informational materials exception applied to "the importation from any country" and also "the exportation to any country."[85] The House report accompanying the 1988 amendment explained: "[T]he principle [is] that no prohibitions should exist on imports to the United States of ideas and information if their circulation is protected by the First Amendment. That principle applies with equal force to the exportation of ideas and information from this country to the rest of the world."[86]

Over the years, the entity charged with administering sanctions under IEEPA, the Treasury Department's Office of Foreign Assets Control, interpreted the informational materials exception narrowly.[87] In 1994, Congress clarified that this exception applies to electronic transmissions, thus limiting the President's power over informational materials transmitted electronically. The 1994 amendment expanded the Berman Amendment "to restrict the Executive from regulating transactions concerning informational materials 'regardless of format or medium of transmission.'"[88] The amendment's evocative title, the "Free Trade in Ideas Act," made plain Congress's intent to embrace cross-border information flows.

Notwithstanding the informational materials exception, IEEPA is the principal authority under which a 2019 Executive Order on information and communications technology and later executive orders targeting TikTok and WeChat were promulgated, as described below.[89]

What were once "sweeping powers over exports, imports, and private financial transactions"[90] granted by IEEPA have now been enlarged further to cover data. The most direct assertion of executive powers over data flows arose through a

---

clear that the legislation sought to remove "barriers that inhibit the free exchange of ideas across international frontiers." 132 CONG. REC. 6550 (1986) (statement of Sen. Charles Mathias, Jr.). Senator Mathias quoted President Ronald Reagan, who had inveighed against real border walls: "Expanding contacts across borders and permitting a free exchange or interchange of information and ideas increase confidence; sealing off one's people from the rest of the world reduce[s] it." *Id.*

84. Senator Mathias argued that "[t]oday's telecommunications media can bring into our living rooms the images and voices of exponents of every political and artistic tendency around the globe. To deny … information entry or exit not only injuries our freedom but insults the intelligence of the American people." 132 CONG. REC. 6551 (1986) (statement of Sen. Charles Mathias, Jr.).

85. 50 U.S.C. § 1702(b)(3).

86. H.R. REP. NO. 100-40, pt. 3, at 113 (1987); *see* Alicia Faison, Note, *TikTok Might Stop: Why the IEEPA Cannot Regulate Personal Data Privacy and the Need for a Comprehensive Solution*, 16 DUKE J. CONST. L. & PUB. POL'Y SIDEBAR 115, 137 (2021).

87. *See* Jarred O. Taylor III, Note, *Information Wants to Be Free (of Sanctions): Why the President Cannot Prohibit Foreign Access to Social Media Under U.S. Export Regulations*, 54 WM. & MARY L. REV. 297, 308 (2012).

88. United States v. Amirnazmi, 645 F.3d 564, 585 (3d Cir. 2011) (quoting Free Trade in Ideas Act, Pub. L. No. 103-236, § 525(c)(1), 108 Stat. 382, 474 (1994) (codified as amended at 50 U.S.C. § 1702)).

89. *See infra* notes 91–92 and accompanying text.

90. Barry E. Carter, *International Economic Sanctions: Improving the Haphazard U.S. Legal Regime*, 75 CALIF. L. REV. 1159, 1164 (1987).

series of executive orders and their implementing regulations across the first Trump Administration and the Biden Administration. While adopted as technical orders focusing on supply chains, rules issued by agencies to implement executive orders may reshape our engagement with the global internet. These relatively obscure corners of federal law give the President enormous hidden power over global personal data flows. In 2019, Executive Order 13873 on "Securing the Information and Communications Technology and Services Supply Chain" declared that if the Commerce Secretary determined that an "information and communications technology or service[] . . . *subject to the jurisdiction* or direction of a foreign adversary . . . pose[d] an unacceptable risk to the national security of the United States," transactions with that service could be banned.[91] Critically, this Order covered not just goods, but services. Furthermore, despite its title as a regulation of the "supply chain," it applied broadly to information and communications technologies and services, whether or not a supply chain was involved.

For example, even though we may not think of TikTok and WeChat as part of a "supply chain," President Trump relied on Executive Order 13873 to ban transactions with TikTok and WeChat in August 2020.[92] Over the subsequent months, however, three federal courts enjoined these bans.[93] On January 5, 2021, President Trump again cited Executive Order 13873 to ban transactions with eight other apps offered by Chinese companies.[94]

Then, on the last day of the first Trump Administration, the Commerce Department issued draft rules to implement Executive Order 13873, which the Biden Administration later largely adopted.[95] This "Supply Chain" Rule seeks to reduce the risk that "data exfiltration" might permit "a foreign adversary to track the locations of Americans, build dossiers of sensitive personal data for blackmail, and conduct corporate espionage from inside the borders of the United States."[96] The Rule empowers the Commerce Secretary to block or require mitigation measures for information and communications technology or services

91. Exec. Order No. 13873, 84 Fed. Reg. 22689, 22689–90 (May 17, 2019) (emphasis added).

92. Exec. Order No. 13942, 85 Fed. Reg. 48637 (Aug. 11, 2020), *revoked by* Exec. Order No. 14034, 86 Fed. Reg. 31423 (June 11, 2021); Exec. Order No. 13943, 85 Fed. Reg. 48641 (Aug. 11, 2020), *revoked by* Exec. Order No. 14034, 86 Fed. Reg. 31423 (June 11, 2021).

93. *See* U.S. WeChat Users All. v. Trump, 488 F. Supp. 3d 912, 930 (N.D. Cal. 2020); TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 86 (D.D.C. 2020); Marland v. Trump, 498 F. Supp. 3d 624, 645 (E.D. Pa. 2020). For a detailed description, see Anupam Chander, Trump v. TikTok, 55 VAND. J. TRANSNAT'L L. 1145, 1156–61 (2022).

94. Exec. Order No. 13971, 86 Fed. Reg. 1249, 1250 (Jan. 8, 2021), *revoked by* Exec. Order No. 14034, 86 Fed. Reg. 31423 (June 11, 2021); *see* Aimen Mir, Nabeel Yousef, Christine Laciak & Colin Costello, *Information and Communications Technology and Services Supply Chain Rule Goes into Effect*, FRESHFIELDS: BLOG (Apr. 9, 2021), https://blog.freshfields.us/post/102gv7s/information-and-communications-technology-and-services-supply-chain-rule-goes-int [https://perma.cc/U6VM-YSF2] ("[T]he Biden administration allowed the Rule to go into effect as scheduled, reportedly to avoid creating any impression that it will be weak on China-related issues.").

95. *See* Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909 (Jan. 19, 2021); Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 17, 2019).

96. 86 Fed. Reg. 4910 (Jan. 19, 2021).

provided by persons "*subject to the jurisdiction*" of a foreign adversary, when, among other things, the service processes sensitive personal data on more than one million U.S. persons and "poses certain undue or unacceptable risks."[97] The Supply Chain Rule marks a broadening of executive branch authority over electronic hardware and digital services.[98]

With Executive Order 14034 on "Protecting Americans' Sensitive Data from Foreign Adversaries" issued on June 9, 2021, the Biden Administration withdrew the specific Trump-era transaction bans with Chinese apps, but directed the Secretary of Commerce to evaluate the threat of "connected software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or *subject to the jurisdiction* or direction of, a foreign adversary."[99]

During its final year in office, the Biden Administration issued another data flow executive order, this one targeting brokerage agreements, vendor agreements, and investment agreements that might give persons from "countries of concern" access to "bulk" U.S. personal data.[100] Executive Order 14117 on "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," issued by the Biden administration on February 28, 2024, sought to regulate the transfer of Americans' bulk sensitive personal data—including genomic, financial, health, and geolocation data, along with biometric identifiers—and government-related data to prevent such information from being accessed by countries of concern and used for espionage purposes or to blackmail government actors.[101] The executive order was implemented through the Data Security Program (DSP), which was announced on December 27, 2024, and went into effect on April 8, 2025.[102] The DSP sets out a new regulatory regime that identifies six countries of concern, including China and Russia, and prohibits a range of data transactions between U.S. entities and the countries of concern themselves, or any "covered persons."[103] The National Security Division of the Department of Justice has been tasked with enforcing the DSP, which also prohibits investment agreements, vendor agreements, and employment agreements between U.S. entities dealing in sensitive personal data and covered persons.[104]

Another critical tool for executive authority to block cross-border data flows is the national security-related review of inbound foreign investments by the Committee on Foreign Investment in the United States (CFIUS). CFIUS is an Executive Branch committee created by statute and chaired by the U.S. Treasury Secretary.[105] In 2018, through the Foreign Investment Risk Review Modernization

97. *Id*. at 4923 (emphasis added).
98. Chander & Schwartz, *supra* note 61, at 2011.
99. Exec. Order No. 14034, 86 Fed. Reg. 31423 (June 11, 2021) (emphasis added).
100. Exec. Order No. 14117, 89 Fed. Reg. 15421 (Mar. 1, 2024).
101. *Id*. at 15421, 15429.
102. *Data Security*, U.S. DOJ: NAT'L SEC. DIV. (Sep. 24, 2025), https://www.justice.gov/nsd/data-security [https://perma.cc/KT8R-ZKTW].
103. 28 C.F.R. §§ 202.601, 202.701 (2025).
104. 28 C.F.R. §§ 202.104, 202.401 (2025).
105. Defense Production Act of 1950, 50 U.S.C. § 4565(k).

Act (FIRRMA), Congress explicitly directed CFIUS to review investments that gave access to "sensitive personal data of U.S. citizens."[106] In 2017, CFIUS review stopped a merger between MoneyGram and Chinese firm Ant Financial due to concerns about data that could identify U.S. citizens.[107] In 2020, Beijing Kunlun Company sold Grindr, an online dating platform, to San Vicente Acquisition after CFIUS raised national security concerns that the Chinese government would be able to use the personal data from the app to blackmail U.S. citizens, including U.S. government officials.[108] In 2020, after a CFIUS review, President Trump barred a Chinese company's acquisition of StayNTouch, a cloud-based hotel management software company, ordering the Chinese company to "refrain from accessing, hotel guest data through StayNTouch."[109] Through Executive Order 14083, the Biden Administration further directed CFIUS to review foreign investment transactions that might result in "the transfer of United States persons' sensitive data to a foreign person."[110]

In April 2024, Congress passed the Protecting Americans from Foreign Adversary Controlled Applications Act in response to, in particular, concerns over Chinese control over the massively popular app, TikTok.[111] This law effectively barred such apps or websites owned by persons from a designated foreign adversary nation from operating in the United States, requiring them to either be shuttered or sold.[112] Control by a foreign adversary is defined to cover situations where foreign persons from the adversary nation own at least twenty percent of the company, directly or indirectly.[113] The law names TikTok specifically, but also allows the President to designate any such entities that operate a website or application (1) where a user can create an account to make, share, and view real-time communications and media; and (2) which has 1,000,000 monthly active users.[114]

Also in April 2024, Congress enacted the Protecting Americans' Data from Foreign Adversaries Act (PADFA) as part of the omnibus bill also containing the

106. Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1703(a)(4)(B)(iii), 132 Stat. 2177, 2178 (2018).

107. Greg Roumeliotis, *U.S. Blocks MoneyGram Sale to China's Ant Financial on National Security Concerns*, REUTERS (Jan. 3, 2018, at 20:04 EST), https://www.reuters.com/article/business/us-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concern-idUSKBN1ET039.

108. Jay Peters, *Grindr Has Been Sold by Its Chinese Owner After the US Expressed Security Concerns*, VERGE (Mar. 6, 2020, at 13:26 EST), https://www.theverge.com/2020/3/6/21168079/grindr-sold-chinese-owner-us-cfius-security-concerns-kunlun-lgbtq [https://perma.cc/3A3R-BXUB].

109. Regarding the Acquisition of StayNTouch, Inc. by Beijing Shiji Information Technology Co., Ltd., 85 Fed. Reg. 13719 (Mar. 10, 2020); *see* Swanson, *supra* note 41.

110. Exec. Order No. 14083, 87 Fed. Reg. 57369, 57373 (Sep. 20, 2022).

111. *See* Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, § 2(g)(3), 138 Stat. 955, 958–59 (2024) (codified in part at 15 U.S.C. § 9901). We discuss the TikTok law and the constitutional challenges it faced in Section II.A below.

112. *See* § 2(a), 138 Stat. at 955–56; § 2(b), 138 Stat. at 956; § 2(c)(1), 138 Stat. at 956–57. The nations named as foreign adversaries are China, Iran, North Korea, and Russia. 10 U.S.C. § 4872(d)(2).

113. § 2(g)(1), 138 Stat. at 958.

114. §§ 2(g)(2)–(3), 138 Stat. at 958–59. Entities that operate a website or application with the primary purposes of product, business, or travel reviews and information are excluded from the definition of "covered entity." § 2(g)(2)(B), 138 Stat. at 958.

TikTok Law.[115] This law makes it illegal "for a data broker to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual" to a foreign adversary country, or any entity controlled by such a country.[116]

B. CHINA

China invented the national security internet. What we call the Great Firewall of China was designed, like its namesake, to protect China from foreign attack—in the form of unwelcome ideas that undermined national order.[117] Its central aim was to filter material available inside China by regulating what was allowed online, as well as "stemming the virtual flow of unfiltered information into the country."[118] The Chinese Communist Party hoped to make China's Internet "nothing less than a 'spiritual garden'. . .—an ennobling space where netizens complete their transformation into perfect citizens."[119] The Ministry of Public Security initiated the Golden Shield Project in the mid-1990s, focused on "filtering specific content for individuals in an expansive surveillance system."[120] As James Fallows has written, the Chinese "[i]nternet came with choke points built in."[121] U.S. providers were not trusted to engage in the censorship that the Chinese Communist Party sought, and thus, access to Facebook, Twitter, and Wikipedia was blocked by the Chinese government.[122]

---

115. *See* Protecting Americans' Data from Foreign Adversaries, 15 U.S.C. § 9901; *see also* Protecting Americans' Data from Foreign Adversaries Act, Pub. L. No. 118-50, 138 Stat. 960 (2024).

116. 15 U.S.C. § 9901(a).

117. Jyh-An Lee & Ching-Yi Liu, *Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China*, 13 MINN. J.L. SCI. & TECH. 125, 129–33 (2012) (noting that "China is obviously not the only country that filters out politically sensitive content" and that "[o]ther countries with similar motives include Bahrain, Ethiopia, Libya, Iran, Indonesia, Malaysia, Myanmar, Thailand, Pakistan, Saudi Arabia, Singapore, Syria, Tunisia, Uzbekistan, and Vietnam").

118. Lorand Laskai, *'Nailing Jello to a Wall,' in* CONTROL 194–95 (Jane Golley, Linda Jaivin & Luigi Tomba eds., 2017). Its official Chinese name, the "Golden Shield" vividly captured this intent to protect against foreign intrusion.

119. *Id.* at 202. We can see hints of this in the didactic videos offered to Chinese youth by Douyin, ByteDance's Chinese counterpart of TikTok—a reality that has been portrayed as an insidious effort by ByteDance to build up Chinese youth while corrupting American youth with less educational fare. Rikki Schlott, *China Is Hurting Our Kids with TikTok but Protecting Its Own Youth with Douyin*, N.Y. POST (Feb. 26, 2023, at 13:42 ET), https://nypost.com/2023/02/25/china-is-hurting-us-kids-with-tiktok-but-protecting-its-own [https://perma.cc/9M6Z-ZB76].

120. Emily Quan, *Censorship Sensing: The Capabilities and Implications of China's Great Firewall Under Xi Jinping*, 39 SIGMA: J. POL. & INT'L. STUD. 19, 20 (2022); *see also* Laskai, *supra* note 118, at 194.

121. James Fallows, *"The Connection Has Been Reset"*, THE ATLANTIC, Mar. 2008, at 66, https://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650. The Chinese government sought to block "foreign ideas [from] flooding into China." MICHAEL KEANE, HAIQING YU, ELAINE JING ZHAO & SUSAN LEONG, CHINA'S DIGITAL PRESENCE IN THE ASIA-PACIFIC: CULTURE, TECHNOLOGY AND PLATFORMS 49 (2021).

122. Min Jiang, *Authoritarian Informationalism: China's Approach to Internet Sovereignty*, 30 SAIS REV. INT'L AFFS. 71 (2010) (noting that "[m]ajor Internet services like Twitter, Facebook, YouTube, and Blogger are still blocked"); *Wikipedia Blocked in China in All Languages*, BBC (May 14, 2019), https://www.bbc.com/news/technology-48269608 [https://perma.cc/FG6U-UEW9] ("All language editions of Wikipedia have been blocked in mainland China since April [2019], the Wikimedia foundation has confirmed.").

Over the last decade, the Great Firewall of China has expanded decisively from worries over intrusion alone to encompass exfiltration. This required a substantial revision of the laws and regulations of the internet.[123] This Section traces the dramatic evolution of Chinese internet regulation at the border from the importation of harmful information to strict controls over data outflows.

A 2010 white paper on the "Internet in China" from the Information Office of the State Council of the People's Republic of China centered internet security as a key feature of internet management.[124] But even here, the internet security concerns focused on the dissemination of information harmful to the people or the state:

> [N]o organization or individual may . . . disseminate information . . . damaging state honor and interests; instigating ethnic hatred or discrimination and jeopardizing ethnic unity; jeopardizing state religious policy, propagating heretical or superstitious ideas; spreading rumors, disrupting social order and stability; disseminating obscenity, pornography, gambling, violence, brutality and terror or abetting crime; humiliating or slandering others, trespassing on the lawful rights and interests of others; and other contents forbidden by laws and administrative regulations.[125]

Cybersecurity, as understood in this white paper, thus accorded with the Golden Shield's goal of cultivating citizens through a controlled information environment.

The focus on cybersecurity as a critical component of national security became clear in 2014 when President Xi Jinping himself headed the Central Leading Small Group for Cybersecurity and Informatization.[126] During the first meeting, "[President] Xi Jinping pointed out that without cybersecurity, there can be no national security, and without informatization, there can be no modernization."[127]

---

123. *See, e.g.*, Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017, at 10:56 EST), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect [https://perma.cc/L2UZ-NFB3] (describing key highlights in China's evolving cyber governance framework).

124. INFO. OFF. OF THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA, THE INTERNET IN CHINA (June 8, 2010), https://us.china-embassy.gov.cn/eng/zt/bps/201206/t20120621_4911374.htm. The white paper's language about information flows has some similarities to the Japanese Prime Minister Shinzo Abe's concept of "free flow with trust," which has been broadly embraced across the world: "Secure information flow. The free and safe flow of Internet information is integrated as a whole. On the premise of protecting the safe flow of Internet information, the free flow of Internet information may be realized." *Id.*; *see Speech by Prime Minister Abe at the World Economic Forum Annual Meeting*, MINISTRY OF FOREIGN AFFS. OF JAPAN (Jan. 23, 2019), https://www.mofa.go.jp/ecm/ec/page4e_000973.html [https://perma.cc/ZE9Y-NDVC].

125. INFO. OFF. OF THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA, *supra* note 124.

126. Shannon Tiezzi, *Xi Jinping Leads China's New Internet Security Group*, THE DIPLOMAT (Feb. 28, 2014), https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group [https://perma.cc/MUU5-68JQ].

127. *The First Meeting of the Central Network Security and Informatization Leading Group Was Held and Xi Jinping Delivered an Important Speech*, CYBERSPACE ADMIN. OF CHINA (Feb. 27, 2014, at 21:08 EST), http://www.cac.gov.cn/2014-02/27/c_133148354.htm [https://perma.cc/SEZ7-HUWC];

Somewhat surprisingly, he simultaneously recognized the importance of cross-border data flows, noting that "[n]etwork information flows across borders, and information flow leads technology flow, capital flow, and talent flow."[128] Of course, "online public opinion guidance" would remain a touchstone of the Chinese government's approach, he declared.[129] The National Security Law adopted the following year, 2015, introduced a national security review of "key technologies and network information technology products and services."[130]

The reorientation of the Great Firewall to control outward flows took its contemporary shape the following year.[131] In 2016, the Standing Committee of the Chinese National People's Congress adopted the Cybersecurity Law, which introduced a category of "Critical Information Infrastructure" operators.[132] The law explained the type of information that was to be protected by such entities: that which, "if destroyed, suffering a loss of function, or experiencing leakage of data," would "seriously endanger national security, national welfare, the people's livelihood, or the public interest."[133] Most importantly, Critical Information Infrastructure operators would face a data localization obligation, such that the personal data and important data they collect or produce be stored in China, and transferred overseas only after a security assessment.[134] "Critical Information Infrastructure" was left undefined in the statute, though it would include "public communication and information services."[135] The focus on communications platform operators reflects the government's ongoing concern with social and political stability.[136]

---

see also Sacks, *supra* note 123 (describing China's cybersecurity law "as the 'keystone in an arch' of the Xi government's larger buildout of a legal framework for security controls in cyberspace").

128. Matthew Johnson, *China's Grand Strategy for Global Data Dominance*, *in* 2 CHINA'S GLOBAL SHARP POWER, OCCASIONAL PAPER SERIES 24 (Larry Diamond, Glenn Tiffert & Frances Hisgen eds., 2023), https://www.hoover.org/sites/default/files/research/docs/Johnson_ChinasGrandStrategy_Web.pdf.

129. Cyberspace Administration of China, *supra* note 127.

130. Ngoc Son Bui & Jyh-An Lee, *Comparative Cybersecurity Law in Socialist Asia*, 55 VAND. J. TRANSNAT'L L.631, 638–39 (2022); *see* Zhonghua Renmin Gongheguo Guojia Anquan Fa (中华人民共和国国家安全法) [China's National Security Law] (promulgated by the Standing Comm. Nat'l People's Cong., July 1, 2015, effective July 1, 2015), art. 59, *translated in National Security Law of the People's Republic of China*, WORDPRESS: CHINA COPYRIGHT & MEDIA (Rogier Creemers ed., July 2, 2015), https://chinacopyrightandmedia.wordpress.com/2015/07/01/national-security-law-of-the-peoples-republic-of-china [https://perma.cc/AP6V-VATN].

131. The Chinese government apparently decided not to require data localization in its Counterterrorism Law in 2015. Jyh-An Lee, *Hacking into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 66 (2018) ("The Chinese government . . . planned to require data localization in the Counterterrorism Law but removed the provision from its final draft in December 2015.").

132. Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China] (adopted by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 34, *translated in Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, STAN. UNIV.: CYBER POL'Y CTR.: DIGICHINA (Roger Creemers, Graham Webster & Paul Triolo eds., June 29, 2018), https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017 [https://perma.cc/AP75-H5NW].

133. *Id*. at art. 31.

134. *Id*. at art. 37.

135. *Id*. at art. 31.

136. *See* Rogier Creemers, *Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century*, 26 J. CONTEMP. CHINA 85, 95 (2017) (discussing how "[t]he reorganization of China's Internet governance apparatus was largely justified through broadly defined threats

The data localization obligation was arguably "the most controversial provision" of the Cybersecurity Law.[137] Thus, the definition of Critical Information Infrastructure and the details of the security assessment for data exports were particularly salient to businesses across the world.[138] On July 7, 2022, the Cyberspace Administration of China adopted measures requiring government approval in the following cases before transferring data abroad:

> Personal information and important data collected and produced by critical information infrastructure operators; [w]here the data transferred abroad contains important data; [p]ersonal information handlers handling the personal information of over 1 million people providing personal information abroad; [c]umulative provision abroad of the personal information of more than 100,000 people or the sensitive personal information of more than 10,000 people; [and o]ther circumstances [specified by] the State cybersecurity and informatization department.[139]

The data export security assessment can be met through a security certification from entities designated by the Cyberspace Administration of China.[140] In 2022, the secretariat of the National Information Security Standardization Technical Committee published the Specifications on Security Certification for Cross-Border Personal Information Processing Activities.[141] The specifications borrow a feature of European law—what the EU calls "binding corporate rules," that is, special rules for information transfer among corporate affiliates.[142] The Personal Information Protection Law (PIPL) also borrows European practice by permitting

---

to the stability of the regime"); Geoffrey Hoffman, *Cybersecurity Norm-Building and Signaling with China*, *in* GOVERNING CYBERSPACE: BEHAVIOR, POWER AND DIPLOMACY 187, 189 (Dennis Broeders & Bibi van den Berg eds., 2020) (discussing how "China uses censorship as a cybersecurity tool").

137. Gabriela Kennedy & Xiaoyan Zhang, *China Passes Cybersecurity Law*, 29 INTELL. PROP. & TECH. L.J. 20, 20 (2017); *see also* Lee, *supra* note 131, at 79.

138. *See* Lee, *supra* note 131, at 79.

139. Shùjù chūjìng ānquán pínggū bànfaõ (zhēngqiú yìjiàn gaõo) (数据出境安全评估办法 (征求意见稿)) [Measures for Security Assessment of Cross-Border Data Transfer (Draft for Public Comment)] (promulgated by the Cyberspace Admin. of China, Nov. 28, 2021), art. 4, *translated in* Creemers et al., *supra* note 2; *see* Shùjù chūjìng ānquán shěnchá bànfaõ (数据出境安全审查办法) [Measures for Security Assessment of Outbound Data Transfer] (promulgated by the Cyberspace Admin. of China, June 24, 2022, effective Sep. 1, 2022), art. 4, *translated in* Rogier Creemers, Graham Webster, Samm Sacks & Lorand Laskai, *Translation: Outbound Data Transfer Security Assessment Measures – Effective Sept. 1, 2022*, STAN. UNIV.: CYBER POL'Y CTR.: DIGICHINA (July 8, 2022), https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022 [https://perma.cc/QAQ6-ZCSC]. The focus on volume of personal data can be found in U.S. law as well. *See, e.g.*, *supra* note 97 and accompanying text.

140. *See* Lester Ross, *China Updates Specification on Security Certification for Cross-Border Personal Information Processing Activities*, WILMERHALE (Jan. 4, 2023), https://www.wilmerhale.com/insights/client-alerts/20230104-china-updates-specification-on-security-certification-for-crossborder-personal-information-processing-activities [https://perma.cc/DL4X-LJGM].

141. The first version was published in June 2022, and a second version on December 16, 2022. *See id.*

142. Amigo L. Xie, Susan Munro, Xiaotong Wang, Yibo Wu & Prudence Pang, *What You Need to Know About China 'Binding Corporate Rules' Under the New Certification Specifications*, NAT'L L. REV. (July 22, 2022), https://www.natlawreview.com/article/what-you-need-to-know-about-china-binding-corporate-rules-under-new-certification [https://perma.cc/6Z88-VZZV] (noting that

standard contractual clauses and certification mechanisms for data transfers abroad.[143] In 2023, the Cyberspace Administration of China finalized rules for Standard Contractual Clauses for Cross-border Transfers of Personal Information.[144] These rules provide a template "standard contract" designed to facilitate cross-border transfer of personal information.[145]

In 2021, China further elaborated the cybersecurity framework through the Data Security Law.[146] Where parts of the PIPL framework borrowed from the GDPR, the Data Security Law was "generally seen as a response to the U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act)."[147] The Data Security Law establishes a new category of "core data," defined as any data that concerns Chinese national and economic security, Chinese citizens' welfare, and significant public interests.[148] "Important data" is the next-most sensitive level of data, with its scope elaborated in the 2024 Regulations on Network Data Security Management, to refer to data that "could directly threaten national security, economic stability, social order or public health and safety."[149] The Data Security Law embraces the "free flow of data" as long as it occurs in a "lawful and

an applicant for a certification may include a "China-based entity within [a multi-national corporation] or a Group of Undertakings").

143. *Consumer Data Privacy: EU's GDPR vs. China's PIPL*, BLOOMBERG L. (May 3, 2023), https://pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-eus-gdpr-vs-chinas-pipl; *see* Matthew S. Erie & Thomas Streinz, *The Beijing Effect: China's Digital Silk Road as Transnational Data Governance*, 54 N.Y.U. J. INT'L L. & POL. 1, 30–31 (2021).

144. Amigo L. Xie & Prudence Pang, *China Standard Contract that Impacts Transferring Personal Information from China*, K&L GATES (July 20, 2023), https://www.klgates.com/China-Standard-Contract-That-Impacts-Transferring-Personal-Information-From-China-7-20-2023 [https://perma.cc/PT4J-S3Q2].

145. *Id.*

146. *See* Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong. Gaz., June 10, 2021, effective Sep. 1, 2021) [hereinafter Data Security Law of the People's Republic of China], *translated in Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*, STAN. UNIV.: CYBER POL'Y CTR.: DIGICHINA (June 29, 2021), https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china [https://perma.cc/YQG4-B68E].

147. Ryan D. Junck et al., *China's New Data Security and Personal Information Provision Protection Laws: What They Mean for Multinational Companies*, SKADDEN (Nov. 3, 2021), https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws [https://perma.cc/D8V7-43ZV].

148. Waõngluò shùjù ānquán guaõnlǐ tiáolì (yìjiàn gaõo) (网络数据安全管理条例 (意见稿)) [Online Data Security Management Regulations (Draft for Comment)] (promulgated by the Cyberspace Admin. of China, Nov. 14, 2016), art. 73, *translated in* Rogier Creemers, Hunter Dorwart & Graham Webster, *Translation: Online Data Security Management Regulations (Draft for Comment) – Nov. 2021*, STAN. UNIV: CYBER POL'Y CTR.: DIGICHINA (Dec. 6, 2021), https://digichina.stanford.edu/work/translation-online-data-security-management-regulations-draft-for-comment-nov-2021 [https://perma.cc/HWK2-FJUB]; *see also* Josh Horwitz, *China Drafts New Data Measures, Defines "Core Data,"* REUTERS (Sep. 30, 2021, at 06:45 EDT), https://www.reuters.com/world/china/china-issues-draft-rule-data-security-industry-telecoms-2021-09-30.

149. LIZA L.S. MARK & TIANYUN (JOYCE) JI, HAYNES BOONE, CHINA RELEASES REGULATIONS ON NETWORK DATA SECURITY MANAGEMENT (2024), https://www.haynesboone.com/~/media/Project/HaynesBoone/HaynesBoone/PDFs/Alert%20PDFs/2024/China%20Update%2038%20%20China%20Releases%20Regulations%20on%20Network%20Data%20Security%20Management [https://perma.cc/P2NU-BUZ5].

orderly" manner.[150] The law also serves as a blocking statute against requests for data made by foreign authorities, permitting such transfers only with approval of the competent Chinese authorities.[151]

In March 2024, seemingly in response to widespread business worries about the difficulties of transferring data abroad, the Cyberspace Administration of China released "Regulations on Promoting and Regulating Cross-Border Data Flows."[152] The Regulations introduced important exceptions to the requirement for data security assessment, including for transfers of information about less than 100,000 persons and transfers required to fulfill contracts or for human resources management.[153] Overall, we see the Chinese government seeking to control outward flow of data that might undermine national security, while trying to reduce the harm to commerce that such controls entail through special mechanisms for outward transfer.

C. THE EUROPEAN UNION

Like China and the United States, the European Union, too, has erected digital barriers to exports of data in order to protect against foreign surveillance. But, unlike China and the United States, the Digital Berlin Wall of Europe seeks not to protect European national security, but rather safeguard the fundamental rights of European Union residents against foreign national security-based surveillance.[154] Yet, paradoxically, this commitment to rights-based protection may render Europe's Digital Berlin Wall as formidable as the Great Firewall of China and the U.S. Digital Wall.

---

150. Data Security Law of the People's Republic of China, art. 7.

151. *Id*. at art. 36.

152. *China Relaxes Security Review Rules for Some Data Exports*, REUTERS (Mar. 22, 2024, at 14:18 PDT), https://www.reuters.com/technology/cybersecurity/chinas-cyberspace-regulator-issues-rules-facilitate-cross-border-data-flow-2024-03-22 (noting that the new rules finalized an earlier proposed relaxation of regulations that had been "greeted with relief by foreign and Chinese firms in China that trade outside the country").

153. Guaõngquāng Kuàbiān Shùjù Liúdòng Guīdìng (促进和规范跨境数据流动规定) [Provisions on Promoting and Standardizing Cross-Border Data Flows] (promulgated by Cyberspace Admin. of China, Mar. 22, 2024), art. 5, https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm [https://perma.cc/W4AS-G4N5]; Bob Li, *China Released New Regulations to Ease Requirements for Outbound Cross-Border Data Transfers*, WHITE & CASE (Apr. 2, 2024), https://www.whitecase.com/insight-alert/china-released-new-regulations-ease-requirements-outbound-cross-border-data-transfers [https://perma.cc/B3TQ-EYJF]; Lisa M. Ropple et al., *China Finalizes Provisions on Cross-Border Data Transfer*, JONES DAY (Mar. 29, 2024), https://www.jonesday.com/en/insights/2024/03/china-finalizes-provisions-on-crossborder-data-transfer [https://perma.cc/3JD4-UMJT]; *see also* Waõngluò Shùjù Ānquán Guaõnlǐ Tiáolì (网络数据安全管理条例) [Regulations on Network Data Security Management] (promulgated by the State Council, Sep. 30, 2024, effective Jan. 1, 2025), State Council Decree No. 790, https://www.gov.cn/zhengce/content/202409/content_6977766.htm [https://perma.cc/X8DX-45WV] (further clarifying data security obligations, including for foreign providers processing Chinese data).

154. Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, 8 PENN. ST. J.L. & INT'L AFFS. 49, 108 (2020) (discussing how "the EU is compelled to adopt a high level of data protection because it is guaranteed as a fundamental right within its legal system").

The European Union established cross-border data flow restrictions early on, as a means to ensure that its data protection rules could not be readily circumvented by the expedient of transferring data processing overseas.[155] Limiting outbound (but not inbound) flows protected against improper data processing of personal information.[156] This was, of course, the opposite of the early Chinese approach, which placed constraints on inbound information flows, but not outbound flows.[157] These cross-border data transfer rules sought to ensure that the personal data of Europeans was collected, processed, and retained according to the rules set out in European law.[158] The national security turn in these laws is relatively recent, at least at the regional level.

In 2020, in the famous case of *Data Protection Commissioner v. Facebook Ireland Ltd. & Maximillian Schrems* (*Schrems II*), the Court of Justice of the European Union declared that the principal mechanism for personal data transfer to the United States—standard contractual clauses—was insufficient, and that the European Commission's adequacy ruling for U.S. data protection for companies complying with the EU–US Privacy Shield was invalid.[159] As the Court explained, "those clauses are not capable of binding the authorities of that third country, since [the authorities] are not party to the contract."[160] Instead, the Court directed that transfers to countries without a data protection regime judged as adequate could occur only with "the adoption of supplementary measures."[161] The decision in the case, though rooted in European data protection law, was ultimately based on the Court's assessment of U.S. surveillance law, specifically the Foreign Intelligence Surveillance Act, Executive Order 12333, and Presidential Policy Directive 28.[162] The "largely unrestrained surveillance regime, a lack of redress under that regime, and the lack of independence for the ombudsperson" meant that the privacy of European data subjects would not be sufficiently protected if their data arrived in the United States, the Court concluded.[163]

It would take three years for the United States to negotiate a successor arrangement to the Privacy Shield. During that time, the Berlin data protection authority issued guidance on video conferencing, offering a "traffic light" assessment of data protection issues in some common software, placing Cisco, Microsoft, Google, Skype, and Zoom under "red lights," while rating smaller, German

155. *See* Directive 95/46/EC, European Union Data Protection Directive, 1995 O.J. (L 281), Chapter IV, 45–46.

156. *See* Chander & Schwartz, *supra* note 60, at 91.

157. *See* Quan, *supra* note 120, at 26.

158. Council Regulation 2016/679 of Apr. 27, 2016, European Union Data Protection Directive, 2016 O.J. (L 119), art. 25 [hereinafter European Union Data Protection Directive].

159. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximillian Schrems, ECLI:EU:C:2020:559, 2020 E.C.R. I-559, ¶¶ 60–64 (July 16, 2020) [hereinafter *Schrems II*].

160. *Id.* at ¶ 125.

161. *Id.* at ¶ 133.

162. *Id.* at ¶ 45.

163. Monika Zalnieriute, *Data Transfers after* Schrems II*: The EU-US Disagreements over Data Privacy and National Security*, 55 VAND. J. TRANSNAT'L L. 1, 25 (2022); *see also Schrems II*, 2020 E.C.R. I-559, at ¶¶ 8, 178, 195.

providers "green."[164] The Hamburg and Berlin authorities asked hundreds of companies (such as mail, hosting, tracking, and adtech service providers) to report on data flows.[165] The Berlin authority noted that such an information request led most companies to voluntarily stop data transfers.[166] The administrative court of Wiesbaden temporarily enjoined transfers to Danish cookie consent management provider Cybot because it relied on U.S.-based content delivery network Akamai, and thus might cause data to flow to U.S. servers.[167] However, a state administrative court withdrew the temporary injunction in favor of further consideration.[168] Similarly, an earlier case upholding the blanket exclusion of public hospitals using EU subsidiaries of U.S. cloud service providers on the basis of "latent risk" of access by U.S. agencies was overturned in Baden-Württemberg state court.[169] A Munich court, on the other hand, prohibited the online use of Google Fonts, because that involved transferring IP addresses of European users to Google's servers in the United States.[170] In response, some practitioners advised that companies either locally imbed all forms of tracking technology or abstain from using them.[171] In Austria, where Max Schrems and his None of Your Business (NOYB) non-governmental organization are based, the national data protection authority was the first to hold use of Google

164. BERLINER BEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT [BERLIN AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION], HINWEISE FÜR BERLINER VERANTWORTLICHE ZU ANBIETERN VON VIDEOKONFERENZDIENSTEN [INFORMATION FOR BERLIN OFFICIALS REGARDING PROVIDERS OF VIDEO CONFERENCING SERVICES] 2, at 3–6 (2021) [hereinafter BLNBDI], https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/dokumente/2021-BlnBDI_Dienste-fuer-Videokonferenzen.pdf [https://perma.cc/Z66P-79RK].

165. *Id*. at 1, 2, 33.

166. *Id*. at 16.

167. Stefan Krempl, *Gericht: Deutsche Webseiten Dürfen Keine US-Cookies Setzen* [*Court: German Websites Are Not Allowed to Set U.S. Cookies*], HEISE ONLINE (Dec. 8, 2021, at 00:02 UHR), https://www.heise.de/news/Gericht-Deutsche-Webseiten-duerfen-keine-US-Cookies-setzen-6288818.html [https://perma.cc/6QJU-K9PT].

168. *Hesse: Administrative Court of Hesse Lifts Interim Injunction on RheinMain University for Using Cookiebot*, DATAGUIDANCE (Feb. 1, 2022), https://www.dataguidance.com/news/hesse-administrative-court-hesse-lifts-interim [https://perma.cc/F3FK-XLL4].

169. *See* Vergabekammer Baden-Württemberg [VK Baden-Württemberg] [Baden-Wuerttemberg Public Procurement Chamber] Jul. 13, 2022, 1 VK 23/22 (Ger.), https://openjur.de/u/2447201.html; Oberlandesgericht Karlsruhe [OLG Karlsruhe] [Karlsruhe High State Court] Sep. 7, 2022, 15 Verg 8/22 (Ger.), https://openjur.de/u/2449559.html; *see also* René M. Kieselmann, Mathias Pajunk & Stefan Peintinger, *US-Cloud and DSGVO/OLG Overturns Decision of the Public Procurement Chamber BW*, SKW SCHWARZ (Sep. 20, 2022), https://www.skwschwarz.de/en/news/neuer-beschluss-des-olg-karlsruhe [https://perma.cc/BW7P-5TD9].

170. Landesgericht München [LG München] [Munich State Court] Jan. 20, 2022, 3 O 17493/20, Bayern, https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2022-N-612; Niklas Plutte, *LG München: Einbindung von Google Fonts ohne Einwilligung* [*Munich Regional Court: Integration of Google Fonts Without Consent*], KANZLEI PLUTTE (Aug. 16, 2022), https://www.ra-plutte.de/lg-muenchen-dynamische-einbindung-google-web-fonts-ist-dsgvo [https://perma.cc/4EDT-99T8].

171. *LG München: Google Fonts sind nicht mehr datenschutzkonform* [*Munich Regional Court: Google Fonts Are No Longer Compliant with Data Protection Regulations*], IT-DAILY.NET: ONLINEPORTAL VON IT MANAGEMENT (Aug. 19, 2022, at 10:58 ET), https://www.it-daily.net/it-sicherheit/datenschutz-grc/lg-muenchen-google-fonts-sind-nicht-mehr-datenschutzkonform [https://perma.cc/96PM-S78S].

Analytics unlawful, despite supplemental measures, as access under the Foreign Intelligence Surveillance Act was still possible.[172] On February 10, 2022, the French *Commission nationale de l'informatique et des libertés* (CNIL) followed with a similar judgment, also based on a complaint brought by NOYB.[173] The CNIL ruled that the use of Google Analytics violated the GDPR because personal data was transferred by Google to the United States.[174]

The launch of the EU-U.S. Data Privacy Framework (the Framework) in 2023 offered a mechanism to transfer data to the United States under the umbrella of an adequacy decision.[175] It committed the U.S. government to various protections to avoid the disproportionate collection of data and provided remedies for any violation.[176] However, it alleviates, but does not eliminate, the challenges to transferring data to the United States or using suppliers subject to U.S. jurisdiction. First, any data flow restrictions based on national security laws in the EU's member states are largely unaffected by the Framework. National security is reserved to each of the member states, and thus a review of each member state's national laws would be required to identify any constraints on outbound data flows.[177] Second, the Court of Justice of the European Union could yet find the Framework a violation of Europeans' fundamental rights, and thus it too could be repudiated in the future, like its two predecessor Transatlantic arrangements.[178] The European General Court rejected a challenge to the Data Privacy Framework brought by a French legislator, holding that the applicant had not shown that he personally would be harmed by its continued operation, and that he had not even

172. Datenschutzbehörde Republik Österreich [DSB] [Data Protection Authority of Austria] Dec. 22, 2021, D155.027, No. 2021-0.586.257 (Austria), https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_DE_bk_0.pdf [https://perma.cc/94KT-NU4J]; Caitlin Fennessy, *The Austrian Google Analytics Decision: The Race Is On*, IAPP (Feb. 7, 2022), https://iapp.org/news/a/the-austrian-google-analytics-decision-the-race-is-on [https://perma.cc/22GM-A2UV].

173. Mariné Margaryan, Nancy Libin & John D. Seiver, *Growing Trouble for EU-U.S. Data Transfers Through Google Analytics*, DAVIS WRIGHT TREMAINE LLP (Feb. 22, 2022), https://www.dwt.com/blogs/privacy–security-law-blog/2022/02/google-analytics-gdpr-data-transfers [https://perma.cc/E8R4-GPTZ].

174. Catherine Stupp, *U.S. Companies Face More Restrictions After Privacy Ruling Against Google*, WALL ST. J. (Feb. 1, 2022, at 05:30 ET), https://www.wsj.com/articles/u-s-companies-face-more-restrictions-after-privacy-ruling-against-google-11643711405; Kirk J. Nahra, Martin Braun, Amy Gopinathan & Ali A. Jessani, *The French Data Protection Authority Joins the Austrian Data Protection Authority in Ruling that the Use of Google Analytics Violates the GDPR*, WILMERHALE (Feb. 16, 2022), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20220216-the-french-data-protection-authority-joins-the-austrian-data-protection-authority-in-ruling-that-the-use-of-google-analytics-violates-the-gdpr [https://perma.cc/FGG4-XGRR].

175. *See* Commission Implementing Decision EU 2023/1795, 2023 O.J. (L 231) ¶¶ 2–3, 7–8.

176. *See id.* at ¶¶ 68, 112–18. President Biden issued an Executive Order to implement the framework. Exec. Order No. 14086, 87 Fed. Reg. 62283 (Oct. 14, 2022).

177. *See* Consolidated Version of the Treaty on European Union art. 4(2), May 9, 2008, 2008 O.J. (C 115) 18 ("[N]ational security remains the sole responsibility of each Member State.").

178. *European Commission Gives EU-US Data Transfers Third Round at CJEU*, NOYB (July 10, 2023), https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu [https://perma.cc/K5LD-KFKT]; Laura Kayali, *French Lawmaker Challenges Transatlantic Data Deal Before EU Court*, POLITICO (Sep. 7, 2023, at 19:00 CET), https://www.politico.eu/article/french-lawmaker-challenges-transatlantic-data-deal-before-eu-court [https://perma.cc/MSX8-ETUQ].

provided evidence that he had used Microsoft 365, Google, or Doctolib.[179] Third, the Framework is not applicable to any countries other than the United States, which negotiated a sui generis adequacy regime; other countries might face similar prohibitions on data flows in the future. Finally, the Framework is only applicable to the companies that maintain active certifications under it.[180]

While *Schrems II* itself focuses on the United States,[181] its logic extends to the transfer of personal data to all countries outside the European Union that do not benefit from an adequacy decision. This is most of the rest of the world, as only eleven countries carry an adequacy decision.[182] Hamburg's data protection authority, the relevant authority for Google's operations, suggested that because contractual agreements cannot protect against state authorities, transfers to non-adequate countries "can therefore no longer happen in the future."[183] It specifically noted that China was "far away" from adequacy.[184]

Furthermore, digital sovereignty concerns may still lead some EU jurisdictions to bar foreign service providers. For example, early drafts of the EU cloud security certification scheme insisted that cloud providers have their "registered head office and global headquarters . . . in a Member State."[185] If this proposal had been adopted, it would have "effectively . . . exclude[d] [cloud service providers]

---

179. Will Richmond-Coggan et al., *EU-US Data Privacy Framework Challenge Rejected by EU General Court*, FREETHS (Nov. 21, 2023), https://www.freeths.co.uk/insights-events/legal-articles/2023/eu-us-data-privacy-framework-challenge-rejected-by-eu-general-court [https://perma.cc/L8KX-B5YT]. The court's opinion has not yet been released.

180. *See* 2023 O.J. (L 231) ¶¶ 48–52. More than 2,800 U.S. companies are currently certified. Alex LaCasse, *European Commission Report Reviews Progress of EU-US DPF*, IAPP (Oct. 9, 2024), https://iapp.org/news/a/european-commission-report-reviews-progress-of-eu-us-dpf [https://perma.cc/QF57-ZDCX].

181. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximillian Schrems, ECLI:EU:C:2020:559, 2020 E.C.R. I-559 (July 16, 2020).

182. *See* European Commission Press Release IP/24/161, Commission Finds That EU Personal Data Flows Can Continue with 11 Third Countries and Territories (Mar. 12, 2025, at 16:55 CET), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_161 [https://perma.cc/HK8R-2VMN]. Three decades after the passing of the Data Protection Directive, there are only fifteen jurisdictions with adequacy decisions under the GDPR, four of which are European island territories: the countries of Andorra, Argentina, Canada, Israel, Japan, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States, and Uruguay, as well as the territories and dependencies of Faroe Islands, Guernsey, Isle of Man, and Jersey. *Id.* A mutual adequacy decision between Brazil and the EU is expected to be announced soon. Rosie Harris-Davison, *ANPD Director Says EU Adequacy Decision Is in Final Stages*, LEXOLOGY (July 15, 2025), https://www.lexology.com/pro/content/anpd-director-says-eu-adequacy-decision-in-final-stages.

183. DER HAMBURGISCHE BEAUTFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT [HAMBDI] [HAMBURG AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION], *Schwere Zeiten für den Internationalen Datenaustausch—EuGH Suspendiert Privacy Shield und Bestätigt Standard Vertrags Klauseln* [*Difficult Times for International Data Transfers: ECJ Suspends Privacy Shield and Confirms Standard Contractual Clauses*], at 2 (Jul. 16, 2020), https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Pressemitteilungen/2020/2020-07-16_EuGH_Schrems.pdf [https://perma.cc/A4AZ-SAJA].

184. *Id.*

185. Kenneth Propp, Peter Swire & Josh Fox, *Oceans Apart: The EU and US Cybersecurity Certification Standards for Cloud Services*, EUROPEAN L. BLOG (June 27, 2023), https://europeanlawblog.eu/2023/06/27/oceans-apart-the-eu-and-us-cybersecurity-certification-standards-for-cloud-services [https://perma.cc/A3XB-5WBG].

headquartered outside the EU from seeking 'the *highest* level of . . . certification' on the grounds that such [providers] would not be immune from foreign law."[186] A more recent draft has eliminated this requirement, though the issue remains contested.[187] While a few European companies (especially cloud providers) argue for excluding foreign-headquartered providers in order to promote European digital sovereignty,[188] a coalition of twenty-six European industry associations argues that this requirement would harm European industry, preferring a risk-based approach that focuses on a company's actual practices.[189]

The Digital Berlin Wall is a response to concerns of foreign surveillance raised vividly by the Snowden revelations.[190] While a few European companies stand to benefit from the eviction of foreign players from the digital services market, other companies, as well as consumers, will be harmed due to the loss of competition, a topic to which we turn in Part III below.

D. THE EMERGING DOCTRINE OF IMMUNITY FROM FOREIGN JURISDICTION

In the United States, China, and the European Union, we see the emergence of measures designed to stop the flow of personal data outside the jurisdiction because of the risks of foreign surveillance. Each jurisdiction develops a remarkably similar mechanism to thwart foreign surveillance—immunity from foreign jurisdiction as a condition for providing a local information service. This Section defines this new doctrine and explains its *raison d'etre*.

We can define this emerging doctrine of immunity from foreign jurisdiction as follows: *the requirement that an entity conducting local business not be subject to foreign sovereign compulsion*. The goal is to prevent entities that are somehow bound to follow the commands of a foreign government from being permitted to provide services that might have national security implications. Increasingly, countries demand that data not only be stored locally, but that it be collected, stored, and processed by local companies that are not subject to foreign jurisdiction. This is data localization squared—*local* storage by *local* companies that are not subject to foreign jurisdiction.

---

186. *Id.*

187. *See* John Salmon et al. *EUCS: Controversial Sovereignty Issues Continue to Drive Debate for Cloud Services*, HOGAN LOVELLS (June 12, 2024), https://www.hoganlovells.com/en/publications/eucs-controversial-data-sovereignty-issues-continue-to-drive-debate-around-the-eu-certification-scheme-for-cloud-services [https://perma.cc/9FXD-DVHV] (noting that "the removal of the sovereignty requirement is not necessarily a closed issue").

188. *See* Foo Yun Chee, *Exclusive: Deutsche Telekom, Airbus Slam Plan Allowing Big Tech Access to EU Cloud Data*, REUTERS (Apr. 10, 2024, at 16:35 EDT), https://www.reuters.com/technology/deutsche-telekom-airbus-slam-plan-allowing-big-tech-access-eu-cloud-data-2024-04-10.

189. *See* Foo Yun Chee, *EU Cybersecurity Label Should Not Discriminate Against Big Tech, European Groups Say*, REUTERS (June 17, 2024, at 17:21 EDT), https://www.reuters.com/technology/cybersecurity/eu-cybersecurity-label-should-not-discriminate-against-big-tech-european-groups-2024-06-17.

190. *See* Laurens Cerulus & Hans von der Burchard, *Snowden's Back: Spying Scandal Clouds EU-US Ties Ahead of Biden Visit*, POLITICO (May 31, 2021, at 21:16 CET), https://www.politico.eu/article/edward-snowden-is-back-spying-scandal-disrupts-eu-us-ties-ahead-of-joe-biden-europe-visit [https://perma.cc/F7VA-AXSF].

The reasonable assumption underlying the doctrine is that a company that is subject to foreign jurisdiction could be compelled to follow the law of that jurisdiction, even to the extent of compelling it to betray citizens elsewhere. This is true even if a company sees itself as a "Digital Switzerland," in the nice phrase of Microsoft's President, Brad Smith—that is, neutral with respect to local politics.[191] The difficulty is that despite the best efforts of the corporation to aspire to global citizenship or official neutrality,[192] there may be a lack of trust that the corporation's leadership or ownership will resist pressures from a foreign country.

While the most blunt test for being subject to foreign sovereign compulsion is foreign ownership (with the minimum percent foreign ownership to trigger this doctrine sometimes specified[193] and other times left open), the rules can also test for other markers of susceptibility to foreign governments.

Read in its broadest form, the doctrine of immunity from foreign jurisdiction can sweep in even domestic companies with foreign operations. After all, a local company with significant operations elsewhere might be subject to pressure from the foreign jurisdictions in which it operates. If the rules tolerate local companies with foreign subsidiaries, but not foreign companies with local subsidiaries, they may depend on some implicit understanding of the relationship between the parent and subsidiary. Consider, for example, Deutsche Telekom, which has a significant ownership stake in T-Mobile in the United States.[194] That subsidiary presence in the United States might not imperil Deutsche Telekom's immunity from foreign jurisdiction in Europe because Deutsche Telekom is the parent, not the subsidiary, of a U.S. company.

Each of the jurisdictions surveyed includes what amounts to a blocking statute—barring companies from giving up local persons' data to foreign governments. In the United States, the Electronic Communications Privacy Act (ECPA) functions as a blocking statute, at least with respect to foreign government

---

191. Brad Smith, President, Microsoft Corp., Keynote Address at the RSA Conference 2017: The Need for a Digital Geneva Convention 12 (Feb. 14, 2017) (transcript available at https://cyber-peace.org/wp-content/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf [https://perma.cc/GKB5-SCUF]); *see* Eichensehr, *supra* note 69, at 696.

192. *See* Smith, *supra* note 191, at 13 (discussing how technology companies "need to be clear that [they] will not aid in attacking customers anywhere, regardless of the government that may ask [them] to do so" and "need to make the case to the world that the world needs to retain its trust in technology"); Eichensehr, *supra* note 69, at 680; *see also* Donohue, *supra* note 19, at 23 ("[W]ith the impact of lack of privacy controls in the surveillance sphere on U.S. competitiveness in mind . . . in December 2013, some of the largest U.S. Internet companies launched a campaign to . . . limit government authority to collect user data, to institute better oversight and accountability, to ensure greater transparency about what the government is requesting (and obtaining), to increase respect for the free flow of data across borders, and to avoid political clashes on a global scale.").

193. See, for example, the French secure cloud standard, which specifies that "[t]he share capital and voting rights in the service provider's company must not be, directly or indirectly: individually held at more than 24%; and collectively owned more than 39%" by non-EU persons. ANSSI, *supra* note 14, at § 19.6.b.

194. Andreas Leigers, *Deutsche Telekom Acquires 6.7 Million T Mobile US Shares Significantly Below Market Price*, DEUTSCHE TELEKOM AG (June 10, 2024), https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-acquires-6-7-million-t-mobile-us-shares-significantly-below-market-price-1067800 [https://perma.cc/4DYB-9ARJ].

demands for the contents of U.S. communications.[195] The ECPA permits electronic communication providers to provide information to government entities based on a subpoena or warrant[196]—but only to U.S. government entities.[197] The Chinese Data Security Law also includes a blocking provision barring "[d]omestic organizations and individuals" from transferring data stored in China to "the justice or law enforcement institutions of foreign countries without the approval of the competent authorities of the [People's Republic of China]."[198] In the European Union, *Schrems II*'s interpretation of European fundamental rights limits foreign government access to data.[199]

Thus, a company that operates in two jurisdictions would likely face a difficult choice—comply with the law of its home country and violate the law of another, or vice versa. The doctrine of immunity from foreign jurisdiction responds to the possibility that a foreign-owned company might follow its home country's demand even if that demand violates local law, such as the blocking statute described above. Immunity from foreign jurisdiction often entails what Anthony Colangelo calls an "absolute conflict of laws"—"situations of overlapping laws from different states that contain simultaneous contradictory commands."[200] Such a situation might arise here with the home country ordering the transfer of the foreign data horde, and the other country ordering that the data not be subject

195. Gidari, *supra* note 23 ("[L]aw enforcement outside the U.S. can't get data for their legitimate investigations from U.S. providers because the Electronic Communications Privacy Act (ECPA) prohibits such disclosures; that is, ECPA is a classic blocking statute."); STEPHEN P. MULLIGAN, CONG. RSCH. SERV., R45173, CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT 10 (2018) ("ECPA prohibits service providers from disclosing the content of electronic communications directly to foreign governments absent a statutory exception or a warrant from a federal court."); *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 36 (2017) (statement of Richard Salgado, Director, Law Enforcement and Information Security, Google Inc.), https://judiciary.house.gov/wp-content/uploads/2017/06/Salgado-Testimony.pdf [https://perma.cc/2NNF-XPY3] ("ECPA includes a broad, so-called blocking provision that restricts the circumstances in which U.S. service providers may disclose the content of users' communications to government agencies outside the United States.").

196. 18 U.S.C. § 2703(a)–(b).

197. 18 U.S.C. § 2711(4) ("[T]he term 'governmental entity' means a department or agency of the United States or any State or political subdivision thereof."); *see also* Kate Westmoreland, *The Global Corporate Citizen: Responding to International Law Enforcement Requests for Online User Data*, HARV. UNIV.: J. OF L. & TECH. DIGEST (Aug. 12, 2015), https://jolt.law.harvard.edu/digest/the-global-corporate-citizen-responding-to-international-law-enforcement-requests-for-online-user-data [https://perma.cc/RNW9-64X8] ("Foreign governments cannot obtain user content on their own behalf (either voluntarily or compulsorily). This is because the subpoena and court order processes in ECPA are only available to 'governmental entities.'").

198. Data Security Law of the People's Republic of China, art. 36.

199. Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd., ECLI:EU:C:2020:559, ¶ 185 (July 16, 2020) ("[T]he limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States . . . are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required[] under EU law.").

200. Anthony J. Colangelo, *Absolute Conflicts of Law*, 91 IND. L.J. 719, 719, 727 (2016).

to such transfer.[201] When imposed as a requirement for handling personal data, immunity from foreign jurisdiction seeks to provide assurance that that data will not be commandeered by a foreign government for its own purposes.[202]

It is not surprising that this doctrine has become prominent in the context of personal data. Data transfers are particularly difficult for governments to monitor at a national level because they occur over an array of electronic networks.[203] Corporations, on the other hand, often institute significant controls over their networks to monitor data flows and prohibit large scale data transfers.[204]

The doctrine has yet to be elaborated fully. It is not clear whether the existence of a sister company in a foreign jurisdiction is enough to trigger the doctrine.[205] Or whether a company's capital raising in a foreign jurisdiction suffices to give that jurisdiction enough leverage over that company to demand it to betray another country's citizenry? To take a specific example, does Tencent's minority investment in U.S.-based Epic Games[206] mean that Epic's blockbuster game Fortnite is somehow compromised?

The doctrine of immunity from foreign jurisdiction should be distinguished from the well-recognized U.S. law doctrines of foreign sovereign compulsion, act of state, and sovereign immunity.[207] All are concerned in various ways with the actions of foreign governments. However, the latter doctrines are possible defenses that a party can use from a lawsuit in U.S. (and possibly foreign) courts.[208] For example, consider the *raison d'etre* for foreign sovereign compulsion:

> The underlying rationale behind the doctrine is that if a foreign defendant has no choice but to comply with a foreign sovereign's directive, and if this choice

201. Courts tasked with choosing which law to enforce in absolute conflicts cases largely focus on weighing the competing state interests. *Id.* at 726–27. Here, it seems likely that each country's courts would enforce its own country's laws on the data transfer.

202. *See* ANSSI, *supra* note 14.

203. Paul de Hert & Vagelis Papakonstantinou, *Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?*, 9 I/S: J. L. & POL'Y FOR INFO. SOC'Y 271, 307 (2013).

204. Erie & Streinz, *supra* note 143, at 87 ("Governmental control over data flows depends not just on territorial control over data, which can be achieved through territorial data localization, but it also requires effective control over the corporations that build, operate, and maintain the relevant infrastructure."); *see, e.g.*, Angelina Fisher & Thomas Streinz, *Confronting Data Inequality*, 60 COLUM. J. TRANSNAT'L L. 829, 867–68 (2022) (describing the prevalence of corporate governance of internet data transfer infrastructure).

205. For a discussion of such issues under the CLOUD Act, see Justin Hemmings, Sreenidhi Srinivasan & Peter Swire, *Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act*, 10 J. NAT'L SEC. L. & POL'Y 631 (2020).

206. Press Release, *Tencent Removes Two Directors from Epic Games and Relinquishes Its Right to Unilaterally Appoint Directors or Observers in Response to Justice Department Scrutiny*, DOJ: OFF. OF PUB. AFFAIRS (Feb. 6, 2025), https://www.justice.gov/archives/opa/pr/tencent-removes-two-directors-epic-games-and-relinquishes-its-right-unilaterally-appoint [https://perma.cc/3D6T-YHVN].

207. *See* W.S. Kirkpatrick & Co. v. Env't Tectonics Corp., Int'l, 493 U.S. 400, 405–06 (1990) (distinguishing act of state doctrine from jurisdictional bars).

208. Jane Lee, Note, *Vitamin "C" Is for Compulsion: Delimiting the Foreign Sovereign Compulsion Defense*, 50 VA. J. INT'L L. 757, 763–64 (2010) (discussing the foreign sovereign compulsion defense and related foreign sovereign immunity defense and the act of state doctrine).

> results in a violation of U.S. laws, fairness considerations for the defendant and recognition of the foreign government's interests may outweigh the interests served by holding the foreign defendant liable in a U.S. court.[209]

Immunity from foreign jurisdiction, on the other hand, is not a defense—but a condition for accessing certain privileges offered by the state, namely, the privilege of being able to provide a particular good or service.[210] While the traditional doctrines *privilege* foreign government actions even in domestic proceedings, immunity from foreign jurisdiction is a mechanism to *protect* against foreign government actions.

The fact that there is a logic to the doctrine is, however, not a justification for widespread application of the doctrine to stop cross-border data flows. Part II tracks the doctrine through multiple real-world cases—including literally ripping out foreign company equipment and replacing it with more trusted equipment. Part III will argue that walling off a foreign nation's companies through mechanisms such as a requirement of immunity from foreign jurisdiction may prove counterproductive.

II. CASE STUDIES

A review of recent transnational flashpoints involving the internet demonstrates the broad reach of the national securitization of the internet. They show the national security internet in operation, revealing both its motivations and its costs. They further underscore how internet law is now being written through orders invoking national security and protecting against foreign surveillance. Finally, they highlight the difficulty of disentangling good-faith national security concerns from old-fashioned protectionism.[211]

A. TIKTOK[212]

In March 2024, a month after then-President Joseph Biden joined TikTok,[213] the House Select Committee on the Chinese Communist Party unveiled a bill, with White House support, that would ban TikTok from the United States if it did not sell itself to owners who were not from China.[214] Then-Representative Mike

---

209. *Id.* at 758.

210. *See, e.g.*, CHRISTAKIS, *supra* note 64, at 33 (discussing France's request "to introduce an 'immunity from foreign laws' requirement . . . as a prerequisite to [Cloud Service Providers] seeking 'high level' assurance certification").

211. *Cf.* Heath, *supra* note 55, at 1066–70 (discussing good faith review to control for abuse of measures that harm foreign companies).

212. The author led the submission of two amicus briefs in the case. *See generally* Brief of First Amendment and Internet Law Professors as Amici Curiae in Support of Petitioners, TikTok, Inc. v. Garland, 604 U.S. 56 (2025) (No. 24-656); Brief of First Amendment Law Professors as Amici Curiae in Support of Petitioners, TikTok Inc. & ByteDance, Ltd. v. Garland, 122 F.4th 930 (D.C. Cir. 2024) (No. 24-1113).

213. Madeline Halpert, *'Lol Hey Guys' - Biden Joins TikTok Despite Security Concerns*, BBC (Feb. 12, 2024), https://www.bbc.com/news/world-us-canada-68275634 [https://perma.cc/DX9A-KZXU].

214. SELECT COMM. ON THE CHINESE COMMUNIST PARTY, U.S. HOUSE OF REPRESENTATIVES, TRANSCRIPT OF CHAIRMAN GALLAGHER'S PRESS CONFERENCE RESPONSE TO TIKTOK INTIMIDATION CAMPAIGN AGAINST U. S. USERS (2024), https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house .gov/files/evo-media-document/3.7.24%20Transcript%20of%20Chairman%20Gallagher%E2%80%99s%20Press%

Gallagher, chair of the committee, explained that "we can't take the chance of having a dominant news platform in America controlled or owned by a company that is beholden to the Chinese Communist Party."[215] The rationale for a change in control of the company was the demand for immunity from foreign jurisdiction for a speech platform popular in the United States.[216] The bill sped through the House in nine days with a bipartisan vote.[217] In order to obtain Senate approval, the bill was tied to military aid for Ukraine, Israel, and Taiwan,[218] and was signed into law by President Biden on April 24, 2024.[219]

The TikTok law required that companies no longer distribute TikTok on app stores or provide internet hosting services for TikTok within U.S. borders unless TikTok U.S. was sold.[220] The President would certify a divestiture when Chinese persons, taken together, no longer directly or indirectly own at least a twenty percent stake in TikTok.[221] The law permits the President to declare additional popular social media apps and websites "foreign adversary controlled applications," triggering either a sale or a ban.[222] The law limits legal challenges to the D.C. Circuit Court of Appeals[223] to avoid the plaintiffs seeking a more friendly court and to complicate the fact-finding process. This undermines the traditional judicial check and balance that Koh's National Security Constitution envisions.[224]

20Conference%20Response%20to%20TikTok%20Intimidation%20Campaign%20Against%20U.S.%20Users.pdf [https://perma.cc/5XJ6-F2FJ].

215. *Id.*

216. *Id.*

217. *See All Actions: H.R.7521—118th Congress (2023–2024)*, CONGRESS.GOV, https://www.congress.gov/bill/118th-congress/house-bill/7521/all-actions (noting that the bill was introduced in the House March 5, 2024, and received in the Senate on March 14, 2024) (last visited Dec. 31, 2025); Protecting Americans from Foreign Adversary Controlled Applications Act, H.R. 7521, 118th Cong. (2024).

218. *See* David McCabe & Sapna Maheshwari, *House Moves Towards Bundling TikTok Bill With Aid to Ukraine and Israel*, N.Y. TIMES (Apr. 17, 2024), https://www.nytimes.com/2024/04/17/technology/tiktok-ban-ukraine-israel-aid.html ("By bundling the TikTok legislation with the high-profile aid for Ukraine and Israel, House leaders could force the Senate's hand."); Cristiano Lima-Strong, *Biden Signs Bill That Could Ban TikTok, a Strike Years in the Making*, WASH. POST (Apr. 24, 2024), https://www.washingtonpost.com/technology/2024/04/23/tiktok-ban-senate-vote-sale-biden ("[L]awmakers were able to sidestep a potentially lengthy and contentious debate in the Senate by tying the legislation to passing foreign aid, a cause that already had significant bipartisan backing."); Johanna Costigan, *Congress Speeds TikTok Ban Bill by Adding It to Ukraine, Israel, Taiwan Aid Package*, FORBES (Apr. 19, 2024, at 15:38 EDT), https://www.forbes.com/sites/johannacostigan/2024/04/18/new-legislative-package-proposes-aid-for-ukraine-israel-taiwan-and-banning-tiktok ("Ukraine's access to much-needed assistance hinges on whether or not lawmakers endorse a ban on one particular, albeit popular, social media app.").

219. Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, § 2, 138 Stat. 955, 955–56 (2024).

220. *See* Pub. L. No. 118-50, § 2(a), 138 Stat. at 955–56.

221. *See* Pub. L. No. 118-50, § 2(c)(1), 138 Stat. at 956–57; Pub. L. No. 118-50, § 2(g)(1)(B), 138 Stat. at 958.

222. Pub. L. No. 118-50, § 2(a), 138 Stat. at 955–56.

223. *See* Pub. L. No. 118-50, § 3(a), 138 Stat. at 959–60 (stating that the D.C. Circuit Court of Appeals "shall have exclusive jurisdiction over any challenge to this division or any action, finding, or determination under this division").

224. *See* Koh, *supra* note 30, at 1.

B. "RIP AND REPLACE"

The U.S. government's concerns with Chinese technology companies, of course, go far beyond TikTok. The U.S. government is leading a massive "rip and replace" process for telecommunications hardware from China—literally pulling out equipment manufactured by foreign headquartered companies and replacing it.[225] The "rip and replace" process began in 2019 when the Federal Communications Commission (FCC) launched the Secure and Trusted Communications Networks Reimbursement Program.[226] This program reimburses providers of advanced communications services "for expenses incurred in the removal, replacement, and disposal of communications equipment and services produced or provided by Huawei Technologies Company (Huawei) or ZTE Corporation (ZTE) that [were] obtained on or before June 30, 2020 from their networks."[227] While originally authorized for nearly $2 billion,[228] Congress added $3 billion for the rip and replace program in December 2024.[229]

Programs to rip and replace now extend beyond telecommunications equipment and cover things ranging from drones built by DJI or Autel Robotics to port cranes built by Chinese state-owned company ZPMC.[230]

In 2020, the U.S. Department of the Interior banned procurement by its agencies of drones made by adversary nations, such as China.[231] It lifted its prohibition on nonemergency use after determining that "Interior's security strategy sufficiently mitigated potential risks posed by noncompliant drones."[232] Reviewing these drone restrictions in 2024, the Government Accountability Office (GAO)

---

225. Kelly Hill, *Rip and Replace Funding Passes as Part of Defense Bill*, RCR WIRELESS NEWS (Dec. 18, 2024), https://www.rcrwireless.com/20241218/policy/rip-and-replace-funding [https://perma.cc/J877-S5PG].

226. *Id.*; *Oversight of the Federal Communications Commission: Hearing Before the S. Comm. on Com., Sci. & Transp.*, 116th Cong. 11 (2020) (statement of Ajit Pai, Chairman, Fed. Commc'ns Comm'n) (explaining that the FCC prohibited "recipients [of the Universal Service Fund program] from purchasing equipment or services from companies that pose a national security threat," such as "Huawei and ZTE").

227. SECURE AND TRUSTED COMMUNICATIONS NETWORKS REIMBURSEMENT PROGRAM - SCRP https://fccprod.servicenowservices.com/scrp [https://perma.cc/A3KY-Y55N] (last visited Dec. 31, 2025).

228. Hill, *supra* note 225.

229. Chanda Brown et al., *President Biden Signs the National Defense Authorization Act for Fiscal Year 2025*, COVINGTON: INSIDE GOV'T CONTRACTS (Jan. 2, 2025), https://www.insidegovernmentcontracts.com/2025/01/president-biden-signs-the-national-defense-authorization-act-for-fiscal-year-2025 [https://perma.cc/4DYD-YDL5].

230. *See, e.g.*, Didi Tang, *Congress Is Looking to Ban Chinese Drones That Are Widely Used in US. What to Know About the Debate*, ASSOCIATED PRESS (Dec. 23, 2024, at 08:29 EDT), https://apnews.com/article/china-drones-dji-ban-congress-national-security-09a36a619d2d8a5bd15bb9452774b62c [https://perma.cc/C7X3-5DKQ]; Aruna Viswanatha, Gordon Lubold & Kate O'Keeffe, *Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools*, WALL ST. J. (Mar. 5, 2023, at 11:30 ET), https://www.wsj.com/politics/national-security/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade.

231. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-106924, FEDERAL LANDS: EFFECTS OF INTERIOR'S POLICIES ON FOREIGN-MADE DRONES 1 (2024), https://www.gao.gov/assets/gao-24-106924.pdf [https://perma.cc/7S3U-L8GG].

232. *Id.* at 2–3 (concluding that "the environment in which the department uses its drones is overall of low security risk because these lands are largely accessible to the public and typically removed from areas of national security interest").

concluded that the Bureau of Land Management and the National Parks Service "no longer have enough drones to meet their needs for [wildland fire] operations" and have shifted to "using alternative methods such as helicopters [that] can increase costs and safety risks."[233] Shifting nonemergency operations to alternatives such as crewed aircraft or ground-based methods, rather than drones, can result in the loss of certain advantages drones offer, including higher-quality data, lower costs, reduced safety risks for employees, and diminished disturbance to wildlife and habitats.[234] At the Interior Department, the ban on foreign-made drones has resulted in "reduced collection of data on infrastructure, landscapes and natural resources, and wildlife," according to the GAO.[235] A farmer who uses drones for spraying fertilizer on his crops reported that "[t]he U.S. drones are not as good as DJI ones but cost twice as much."[236] Even the search for lost climbers and hikers might fall victim to these Digital Walls. First responders, from police to search and rescue workers, are pleading with the U.S. government to not ban DJI.[237] The *Wall Street Journal* interviewed the head of air operations for the Weber County Sheriff Search and Rescue team in Utah, who has tested "dozens of drones in the mountains," finding that DJI works the best.[238] "I could not even physically get the American drone to the top of the mountain to begin the search," the search and rescue expert reported.[239] In December 2024, Congress required a national security review of DJI drones, which, if not completed, requires a ban on the import of such drones by the end of 2025.[240]

Concerns range from the mountains to the sea. Giant cranes at U.S. ports may be the new "Trojan horse," U.S. officials worry.[241] Cranes built by Chinese state-owned enterprise ZPMC "may be controlled, serviced and programmed from remote locations," according to Rear Admiral John Vann, who is the Commander

233. *Id.* at 2; *see, e.g.*, *id.* at 10 ("[U]sing helicopters for aerial ignition involves three personnel flying close to the ground, potentially in low-visibility conditions, presenting significantly more risk to personnel compared with drones.").

234. *Id.* at 11–12.

235. *Id.* at 12; *see also* Tang, *supra* note 230 (discussing how domestic drones are not "anywhere close to the DJI drones in terms of reliability, ease of use, and . . . the user-friendly software" (internal quotation marks omitted)).

236. Tang, *supra* note 230.

237. *See* Heather Somerville, *Why First Responders Don't Want the U.S. to Ban Chinese Drones*, WALL ST. J. (Aug. 7, 2024, at 15:10 ET), https://www.wsj.com/politics/national-security/congresss-plan-to-outlaw-chinese-drones-met-with-protest-c95cf1fe.

238. *Id.*

239. *Id.* (internal quotation marks omitted).

240. Chance Townsend, *Have DJI Drones Been Banned in the United States? Not Officially. Not Yet.*, MASHABLE (July 29, 2025), https://mashable.com/article/are-dji-drones-banned [https://perma.cc/RM8Q-R4G5].

241. Viswanatha et al., *supra* note 230. "Trojan horse" was also the term used against TikTok in Congressional debates. *See, e.g.*, Senator Marco Rubio, *TikTok Is a Trojan Horse Living Inside Our Country*, at 02:23, YOUTUBE (Mar. 11, 2024), https://www.youtube.com/watch?v=moFR6z56w0g (then-Senator Marco Rubio calling TikTok a "Trojan horse") (on file with the Georgetown Law Journal).

of the Coast Guard Cyber Command.[242] Then-Chairman of ZPMC explained in 2017 that information flows help the firm to prevent malfunctions by monitoring all the cranes from ZPMC's main office in Shanghai for troubleshooting.[243] ZPMC cranes have been deployed in the United States for two decades, "offering what industry executives described as good-quality cranes that were significantly cheaper than Western suppliers."[244] The U.S. government will spend more than $20 billion in port security, including domestic cargo-crane production, over the next five years.[245] This money would support a U.S. subsidiary of the Japanese company Mitsui to produce cranes in the United States, marking "the first time in 30 years they would be built domestically."[246] The rationale for this expensive endeavor is that the Chinese government could use the cranes to monitor activity at ports, and also to cripple the ports in the event of an international flashpoint between the United States and China.[247]

C. "DELETE AMERICA"

China, for its part, is seeking to remove products from its technology stack that originate from companies subject to U.S. jurisdiction. In 2022, the Chinese government issued Document 79, mandating state-owned enterprises in key sectors like "finance, energy, and other" to replace foreign software with home-grown alternatives.[248] The document is apparently so sensitive that high-ranking officials and executives were not permitted to make a copy of the document and were only allowed to see it.[249] The directive is better known as "Delete A," a reference to "Delete America," as it is largely U.S. software that must be replaced, likely including companies such as Microsoft and Oracle.[250] The Chinese substitutes are sometimes not as good as their foreign alternatives.[251] The push to localize technology ("known as 'Xinchuang,' loosely translated as 'IT innovation'"), is a response to the escalating tech and trade war between the United States and China.[252] While the replacement of foreign chips in Huawei phones has received a great deal of attention,[253] the replacement of foreign software across key public

242. Dustin Volz, Gordon Lubold & Doug Cameron, *U.S. to Invest Billions to Replace China-Made Cranes at Nation's Ports*, WALL ST. J. (Feb. 21, 2024, at 17:10 ET), https://www.wsj.com/politics/national-security/u-s-to-invest-billions-to-replace-china-made-cranes-at-nations-ports-d451ef8f.

243. Viswanatha et al., *supra* note 230.

244. *Id.*

245. Volz et al., *supra* note 242.

246. *Id.*

247. *See id.* (noting U.S. government concern that cranes might allow Chinese government to set off "crippling cyberattacks in the event of a conflict over Taiwan or another flashpoint").

248. Liza Lin, *China Intensifies Push to 'Delete America' from Its Technology*, WALL ST. J. (Mar. 7, 2024, at 00:01 ET), https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f.

249. *See id.*

250. *Id.*

251. *Id.*

252. *Id.*

253. *See, e.g.*, *id.* (discussing Huawei's efforts to replace American technology); Yoko Kubota, *China Bans iPhone Use for Government Officials at Work*, WALL ST. J. (Sep. 6, 2023, at 17:47 ET),

sector operations in China will likely have greater significance for U.S. exports. The underlying theory of Delete A is that foreign software—because it emanates from a foreign enterprise regulated by a foreign government—simply cannot be secure or trustworthy.

But "Delete A" carries a significant price. One commentator described KylinOS, a Chinese alternative to Microsoft's Windows, as "workable if not great," and compared its usability to Microsoft's Windows 7, introduced in 2009.[254] For now at least, Delete A might mean sacrificing more than a decade of progress.

D. MICROSOFT 365

In March 2024, the European Data Protection Supervisor (EDPS) concluded that the European Commission's (the Commission) use of Microsoft 365 had infringed data protection laws for EU institutions and bodies.[255] Why might something as ubiquitous as Microsoft 365 violate data protection law? The EDPS was concerned in part about the transfer of Europeans' personal data outside the EU (or the European Economic Association) to countries not covered by an adequacy decision by the Commission.[256] The EDPS ordered the Commission "to suspend all data flows resulting from its use of Microsoft 365 to Microsoft and to its affiliates and sub-processors, located in third countries not covered by an adequacy decision."[257]

The EDPS seemed to be troubled by the possibility that Microsoft employees or contracted service providers in third countries could remotely access data held on EU servers.[258] The EDPS specified that "remote access from a third country constitutes a transfer" in certain circumstances.[259] Microsoft would have to ensure that all of the relevant employees and service providers accessing EU persons' data were located in the EU or states with adequacy rulings, or otherwise put in place extensive protections against foreign government access to that data—

https://www.wsj.com/world/china/china-bans-iphone-use-for-government-officials-at-work-635fe2f8 (discussing China's directive prohibiting government agency officials from using "Apple's iPhones and other foreign branded devices for work or bring[ing] them into the office").

254. Lin, *supra* note 248.

255. WOJCIECH RAFAL WIEWIÓROWSKI, EUR. DATA PROT. SUPERVISOR, EDPS INVESTIGATION INTO USE OF MICROSOFT 365 BY THE EUROPEAN COMMISSION (CASE 2021-0518) 2 (2024) [hereinafter EUR. DATA PROT. SUPERVISOR]; *see* European Data Protection Supervisor Press Release EDPS/2024/05, European Commission's Use of Microsoft 365 Infringes Data Protection Law for EU Institutions and Bodies 1 (Mar. 11, 2024), https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf [https://perma.cc/R278-C5SN].

256. *See* Richard Speed, *European Commission Broke Its Own Data Privacy Law with Microsoft 365 Use*, THE REGISTER (Mar. 11, 2024, at 13:00 UTC), https://www.theregister.com/2024/03/11/european_commission_infringed_data_protection [https://perma.cc/SMV4-CGAB]; EUR. DATA PROT. SUPERVISOR, *supra* note 255, at 75. For a list of countries labeled adequate, see *infra* note 264.

257. EUR. DATA PROT. SUPERVISOR, *supra* note 255, at 172.

258. *Id.* at 90 (explaining that transfer of personal data through remote access was one of two case scenarios identified by the EDPB "where the EDPB could not identify any effective supplementary measure to ensure . . . protection").

259. *Id.* at 78 (footnote omitted).

what the Court of Justice of the European Union calls "supplementary measures."[260] Supplementary measures are typically adopted following "transfer impact assessments," which evaluate "the level of data protection afforded by the applicable third-country laws" and determine whether supplementary measures are needed.[261] With the adoption of the European Commission's adequacy decision for the United States based on the EU–US Data Privacy Framework,[262] such supplementary measures are no longer necessary for data transfers to the United States,[263] but they remain necessary for countries such as India, Nigeria, or the Philippines, which lack adequacy findings.[264] In this way, these Digital Walls directly affect the ability of workers in the developing world to offer services across the richer parts of the world, undermining a key promise of the internet.[265]

While the EDPS decision only covers the use of Microsoft 365 by the European Commission, it carries significant implications for all companies operating in the European Union. The General Data Protection Regulation (GDPR) rules apply to the private sector as well,[266] and the EDPS decision does not focus on unique aspects of the Commission's use of Microsoft's services. The deficits in the Commission's use of Microsoft 365 would seem to apply to most uses of the service by any EU entity, public or private. And the concerns about 365 would seem to apply to most services that employ service providers outside the EU or countries declared adequate by the Commission itself. The EDPS's decision to investigate the Commission's use of Microsoft 365 and issue a 180-page ruling will likely serve as a warning to others.

By making it more risky, expensive, and cumbersome to use Microsoft 365, the EDPS decision spurs European entities to forego cloud services from foreign providers, possibly undermining cybersecurity as well as other EU goals. As the

260. *See id.* at 101, 106 (noting that under *Schrems II*, "supplementary measures" were necessary for transfers to the U.S. due to inadequate protections against government access and applying this requirement to Microsoft's processing of EU personal data).

261. *Id.* at 88, 147 n.867. Such assessments are central to the EDPS analysis and require reviewing the impact of the cross-border transfer of personal data on fundamental rights, as well as other steps to reduce the risk of foreign government access. *See id.* at 158 ("[T]hird-country legislation to which the processor is subject must respect the essence of the fundamental rights and freedoms recognised by the [EU] Charter and must not exceed what is necessary and proportionate in a democratic society to safeguard . . . important objectives as also recognised in EU or Member State law."). The decision mentions "transfer impact assessment" fifty-seven times. *See id. passim*.

262. EU-US Data Privacy Framework, 2023 O.J. (L 231) 118.

263. European Commission Press Release IP/23/3721, Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows (July 10, 2023), https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

264. *See Adequacy Decisions*, EUROPEAN COMM'N, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/7778-YTMQ] (last visited Dec. 31, 2025) (identifying the sixteen countries that the European Commission has recognized as providing adequate protection).

265. CHANDER, *supra* note 24, at 2 (noting that via the internet, "workers in developing countries . . . participate in lucrative Western markets despite immigration barriers").

266. *The EU General Data Protection Regulation*, HUM. RTS. WATCH (June 6, 2018, at 05:00 EDT), https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation [https://perma.cc/A4H2-JCZE].

European scholar Theodore Christakis notes, "Forcing the European Commission to switch from the cloud . . . to 'on-premise software' by December (if the required corrective measures aren't achievable) is practically impossible for such a massive institution with over 32,000 civil servants . . . ."[267] Christakis goes on to enumerate the problems with the EDPS approach: "[T]his switch would expose the Commission to major issues, including reduced cybersecurity . . . and the inability to use essential services only available on the cloud."[268]

E. CONNECTED CARS

On January 14, 2025, the Department of Commerce announced its final rule for connected vehicles, targeting the import and sale of passenger vehicles containing certain vehicle connectivity systems hardware or software or automated driving software that are manufactured or supplied by persons in China.[269] Modern cars have been described as "smartphones on wheels," and thus "potential spying machines."[270] Concerns include the ability of foreign entities to monitor travels, listen in on conversations, and even to remotely control the car to make it crash.[271] According to the Department of Commerce rule, Chinese made connected vehicles and components pose "undue or unacceptable risks to national security and U.S. persons."[272] The rule thus effectively bars the sale of Chinese cars in the United States, and goes further to require a significant reconfiguration of the global supply chain of automobile parts, which often involve production in China or production elsewhere by Chinese suppliers.[273]

---

267. Theodore Christakis, LINKEDIN, https://www.linkedin.com/feed/update/urn:li:activity:7199405140510957568 [https://perma.cc/7CPB-G6F9] (last visited Dec. 31, 2025).

268. *Id.*

269. Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5360 (Jan. 16, 2025) (to be codified at 15 C.F.R. pt. 791). The law also technically covers Russia. 15 C.F.R. § 791.4 (2025). However, because Russia does not currently have prospects of being a significant car exporter to the United States, various accounts of the rule describe it as focused on China. *See Commerce Finalizes Rule to Secure Connected Vehicle Supply Chains from Foreign Adversary Threats*, U.S. DEP'T OF COM.: BUREAU OF INDUS. & SEC. (Jan. 14, 2025), https://www.bis.gov/press-release/commerce-finalizes-rule-secure-connected-vehicle-supply-chains-foreign-adversary-threats [https://perma.cc/BVQ2-SKSF]. Rulemaking power here stems from Executive Order 13873, issued during the first Trump Administration, which empowered the Secretary to address transactions concerning information and communications technology and services involving foreign adversaries. Exec. Order No. 13873, 84 Fed. Reg. 22689, 22689–90 (May 17, 2019).

270. Kashmir Hill, *'Smartphones on Wheels' Draw Attention from Regulators*, N.Y. TIMES (Apr. 30, 2024), https://www.nytimes.com/2024/04/30/technology/regulators-investigate-carmakers-driver-tracking.html.

271. Lewis, *supra* note 37.

272. Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. at 5366.

273. *See, e.g.*, Qingxiu Bu, *China's Blocking Mechanism: The Unreliable Entity List*, 19 J. INT'L TRADE L. & POL'Y 159, 170 (2020) (explaining how earlier trade tensions between the U.S. and China resulted in "multinational tech companies scrambling to mitigate the disruption to their complex global supply chains"); Jim Tankersley, *Biden Doesn't Want You Buying an E.V. from China. Here's Why*, N.Y. TIMES (May 27, 2024), https://www.nytimes.com/2024/05/27/business/biden-evs.html (discussing how "[c]oncentrating the supply of E.V.s and other advanced green tech in China would risk 'the world's collective ability to have access to the technologies [necessary] . . . to be successful in a clean energy economy'").

The Chinese auto industry association has complained that the rule is designed to prop up American manufacturers rather than enhance national security.[274] But the prohibitions on Chinese products affect not just Chinese manufacturers, but also Mexican, Korean, and even U.S. automakers, which have voiced concerns about the rule. The Mexican government worried that the rule would harm its own automative industry because it relies on parts sourced in China.[275] The South Korean government argued that the rule would "increase[] costs for the automotive industry and place an undue burden on consumers."[276] Waymo, the Alphabet subsidiary that is the leading American self-driving car company in the United States, asserted that federal cybersecurity best practices promulgated by the National Highway Traffic Safety Administration "sufficiently provid[e] state of the art security" for connected vehicles.[277] The Chamber of Progress, an industry association, argued that certain electronic components of self-driving vehicles pose minimal risk, citing the example of LiDAR sensors, which, the group noted, have no need to "connect with their manufacturers or countries of origin."[278] Ford similarly sought to limit the rule to those systems that "genuinely pose the highest potential national security risks."[279] Ford suggested that the rule should focus only on systems that "engage in bidirectional data exchange, have an external internet connection, and have an element of control by a foreign adversary without oversight or compensating controls by a domestic automaker."[280] Ford warned that an overbroad rule would "disrupt U.S. global automotive supply chains."[281] In addition to these economic and supply chain concerns, critics have emphasized that the rule could make it harder for Americans to purchase electric vehicles, thereby discouraging a shift away from fossil fuels and potentially accelerating climate change.[282]

---

274. *See US Proposed Ban on Chinese Connected Vehicles 'May Backfire*,*'* GLOB. TIMES (Jan. 11, 2025, at 01:10 EST), https://www.globaltimes.cn/page/202501/1326662.shtml [https://perma.cc/2HLD-M9ZC]; *China Firmly Opposes U.S. Proposed Ban on Chinese Connected Vehicles*, XINHUA NET (Sep. 25, 2024, at 18:55 ET), https://english.news.cn/20240925/2ee14009551f451d8b98fbbed04176e9/c.html [https://perma.cc/H4X8-YKWV].

275. David Shepardson, *Mexico Warns US Ban on Chinese Car Tech Could Hurt Automotive Industry*, REUTERS (Oct. 28, 2024, at 15:12 EDT), https://www.reuters.com/business/autos-transportation/mexico-raises-concerns-about-us-plan-bar-chinese-vehicle-software-hardware-2024-10-28.

276. Gov't of the Republic of Korea, Comments on the Department of Commerce's Advance Notice of Proposed Rulemaking Regarding Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, at 2 (Apr. 30, 2024).

277. Waymo LLC, Comment Letter on Advance Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, at 12 (Apr. 30, 2024).

278. Chamber of Progress, Comment Letter on Advance Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, at 2 (April 29, 2024).

279. Ford Motor Co., Comment Letter on Advance Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, at 2 (Apr. 30, 2024).

280. *Id.*

281. *Id.*

282. Tankersley, *supra* note 273 (noting that "some environmentalists and liberal economists . . . say the country and the world would be better off if Mr. Biden welcomed the importation of low-cost, low-emission technologies to fight climate change").

Furthermore, banning foreign cars or car parts from a market does not guarantee security. Volkswagen recently suffered a major data exposure when it left several terabytes of unencrypted information gathered from its European cars, including their locations, publicly available on Amazon cloud servers.[283]

F. AI MODELS

During its last week in power, the Biden Administration divided the world into three AI zones with differing levels of access and restrictions.[284] Now we know what countries are within the U.S. Digital Wall, which countries are in the neutral zone, and where the enemy is.[285] The division of the world was operationalized through an obscure rule by the Bureau of Industry and Security (BIS) in the Department of Commerce. The BIS issued its Interim Final Rule on Artificial Intelligence Diffusion ("AI Diffusion Rule"), seeking to control access to AI models for foreign adversary countries.[286] Where earlier efforts had focused on the chips used to power AI systems, this Rule expanded such prohibitions by also targeting AI software, particularly the model weights that are key to the operation of generative AI models.[287] The AI Diffusion Rule limits the foreign transfer of AI model weights for AI models beyond a specified threshold of computational power, unless they are open source models.[288] Even when model weights are permitted to be transferred abroad, they must be transferred to facilities that "are owned or operated by entities headquartered in, or with an ultimate parent headquartered" in acceptable countries.[289] The focus on the country of origin of the parent again shows the immunity from foreign jurisdiction in operation, as the Rule seeks to prevent leakage of the AI model to a company subject to foreign law.

The AI Diffusion Rule would divide the world into Tier 1 countries that face essentially unrestricted access to advanced U.S. AI; Tier 2 states where AI could be transferred with licensing; and Tier 3 countries where advanced AI transfer

283. Patrick Beuth et al., *Massive Data Breach at VW Raises Questions About Vehicle Privacy*, DER SPIEGEL: INT'L (Mar. 1, 2025, at 16:19 UHR), https://www.spiegel.de/international/business/we-know-where-you-parked-massive-data-breach-at-vw-raises-questions-about-vehicle-privacy-a-4b1cb926-2edb-42ea-92fb-5000cd378fc5 [https://perma.cc/Y2AX-433J]; Elisabeth Do, *Real-Case Analysis #56: Volkswagen Data Breach*, CYBERINFO BLOG (Jan. 6, 2025), https://www.cyberinfoblog.com/blog/real-case-analysis-56-volkswagen-data-breach [https://perma.cc/P3Y5-LGKL] ("The breach originated from a misconfiguration in two IT applications managed by Cariad, Volkswagen's software subsidiary.").

284. *See* Framework for Artificial Intelligence Diffusion, 90 Fed. Reg. 4544 (Jan. 15, 2025); *Biden-Harris Administration Announces Regulatory Framework for the Responsible Diffusion of Advanced Artificial Intelligence Technology*, U.S. DEP'T OF COM.: BUREAU OF INDUS. & SEC. (Jan. 13, 2025), https://www.bis.gov/press-release/biden-harris-administration-announces-regulatory-framework-responsible-diffusion-advanced-artificial [https://perma.cc/N7ER-6LVD].

285. The rule grants near-unfettered access for a select roster of trusted nations, imposes a capped, conditional framework for a middle category of countries posing standard and moderate risks under strict licensing constraints, and establishes the most stringent prohibitions—including a presumption of denial for licenses—on countries deemed to pose high risk. 90 Fed. Reg. at 4548.

286. *Id.* at 4544.

287. *Id.* at 4548, 4553–54.

288. *Id.* at 4554.

289. *Id.* at 4565.

would be effectively barred.[290] Only eighteen jurisdictions would find themselves in Tier 1—for example, Canada, Spain, Denmark, and Germany; but Greece, Iceland, and Switzerland would be relegated to Tier 2.[291] Israel, the home of many leading AI enterprises,[292] is not listed in Tier 1, excluded along with most countries in the EU. There are only three countries that have a majority non-white population—Japan, South Korea, and Taiwan.[293] Tier 3 consists of twenty-three countries previously identified as being subject to U.S. arms embargoes.[294] The bulk of the world thus finds itself in Tier 2, subject to significant restrictions both on AI chips and the model weights central to advanced generative AI models. One commentator noted that the Rule seeks "to reshape the international AI landscape,"[295] and another described the rules as "the largest salvo in the new technology cold war."[296] The Rule would, as part of its Tier 2 restrictions, directly affect the AI ambitions of Middle Eastern states such as the United Arab Emirates and Saudi Arabia.[297] An earlier, narrower export control on Nvidia chips resulted in UAE-based G42 "divesting from Chinese firms, stripping out its Huawei technology, and partnering with Microsoft in exchange for access to Nvidia chips."[298] At the same time, John Villasenor observes that "[p]reventing companies in middle-tier countries from relying on the United States to supply computing chips is a surefire way to push them into building non-U.S. alliances that include stronger technology ties with China."[299]

In May 2025, the Trump Administration announced that it was rescinding the AI Diffusion Rule on the grounds that it "stifled American innovation" and undermined relations with foreign countries.[300]

---

290. *Id.* at 4548.

291. *Id.* (listing Australia, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Italy, Japan, the Netherlands, New Zealand, Norway, the Republic of Korea, Spain, Sweden, Taiwan, and the United Kingdom).

292. *See* Kolawole Samuel Adebayo, *AI Companies in Israel Attract 47% of Tech Funding in Major Investment Push*, EWEEK (Nov. 26, 2024), https://www.eweek.com/news/israeli-ai-companies-attract-major-funding/ [https://perma.cc/HZL8-H58G].

293. *See* 90 Fed. Reg. at 4548 (listing countries in Tier 1).

294. *See id.*; 15 C.F.R. pt. 740 (Supp. 1, Aug. 15 2025). The Rule officially describes the Tier 3 countries as "Country Group D:5." 90 Fed. Reg. at 4548. The Rule adds Macau to this list, because the Country Group D:5 treats Macau as a separate jurisdiction from China. *Id.*

295. Sam Winter-Levy, *With Its Latest Rule, the U.S. Tries to Govern AI's Global Spread*, CARNEGIE ENDOWMENT FOR INT'L PEACE: EMISSARY (Jan. 13, 2025), https://carnegieendowment.org/emissary/2025/01/ai-new-rule-chips-exports-diffusion-framework [https://perma.cc/8K7D-U7HN].

296. Dylan Patel et al., *2025 AI Diffusion Export Controls - Microsoft Regulatory Capture, Oracle Tears, Impacts Quantified, Model Restrictions*, SEMIANALYSIS: NEWSLETTER (Jan. 15, 2025), https://semianalysis.com/2025/01/15/2025-ai-diffusion-export-controls-microsoft-regulatory-capture-oracle-tears [https://perma.cc/XQS2-R8Z7].

297. Winter-Levy, *supra* note 295.

298. *Id.*

299. John Villasenor, *The New AI Diffusion Export Control Rule Will Undermine US AI Leadership*, BROOKINGS INST. (Jan. 23, 2025), https://www.brookings.edu/articles/the-new-ai-diffusion-export-control-rule-will-undermine-us-ai-leadership [https://perma.cc/5VLJ-SBUA].

300. *Department of Commerce Announces Rescission of Biden-Era Artificial Intelligence Diffusion Rule, Strengthens Chip-Related Export Control*s, U.S. DEPT. OF COM.: BUREAU OF INDUS. & SEC. (May

III. WEAKNESSES IN DIGITAL WALLS

This Part argues that Digital Walls might prove both costly to maintain and relatively easy to evade. This Part begins by showing that such walls are often ineffective because they do not target the principal means that foreign intelligence services gather personal information—namely, hacking, spying, and buying. This Part then discusses how Digital Walls reduce competition, prove expensive to maintain, and invite retaliation, ultimately undermining one's own enterprises. Furthermore, enforcement of Digital Walls requires significant intrusion into business operations. The final Section argues that national digital security firewalls pose not only the risk of futility but also present a more insidious threat: enhanced government control over the domestic information space and increased opportunities for corruption. These concerns are raised both by the creation of national firewalls and the particular implementation of those firewalls in the form of the requirement of immunity from foreign jurisdiction.

A. INEFFECTIVE: HACKING, SPYING, AND BUYING DATA

Focusing national security efforts on possible foreign sovereign compulsion based on ownership can distract from other ways that governments gather data. After all, foreign intelligence services do not rely only on companies within their jurisdiction to obtain information.[301] They often do not rest on their lawful powers at all.[302] This Section describes three mechanisms often employed to conduct foreign surveillance, beginning with two extra-legal tools: hacking and spying. Foreign intelligence services also employ a third tool, one that may or may not be legal: simply purchasing the data from data brokers.[303] Consequently, malicious foreign actors hardly need to own services in the United States in order to gather information about Americans.

Three examples show the extent of the threat to U.S. national security from foreign hackers likely associated with governments.[304] First, consider the hacking of U.S. federal employee records. The U.S. Office of Personnel Management

13, 2025), https://www.bis.gov/press-release/department-commerce-announces-recission-biden-era-artificial-intelligence-diffusion-rule-strengthens-chip [https://perma.cc/K3UK-CMRS].

301. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 351 (2015).

302. *See, e.g.*, Noah Chauvin, *Too Much Power for Spy Agencies*, BRENNAN CTR. FOR JUST. (Apr. 23, 2024), https://www.brennancenter.org/our-work/analysis-opinion/too-much-power-spy-agencies [https://perma.cc/JA34-9J7C] (discussing how Section 702 of the Foreign Intelligence Surveillance Act was designed "to make it easier for intelligence agencies to spy on foreign terrorists"); Laura K. Donohue, *The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law*, COUNCIL ON FOREIGN RELS. (June 2017), https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law [https://perma.cc/8G4B-DGSP] (arguing that the current use of Section 702 oversteps constitutional bounds).

303. *See* Theodore Rostow, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. ON REGUL. 667, 669, 703 (2017).

304. This Article focuses here on well-known attacks, but it might have enumerated one of the many less well-studied attacks. Consider, for example, the attack on Florida-based software provider Kaseya, whose software was hacked by Russian and Ukrainian criminals to insert ransomware across thousands of companies. Lily Hay Newman, *The Worst Hacks of 2021*, WIRED (Dec. 24, 2021, at 07:00 ET), https://www.wired.com/story/worst-hacks-2021.

(OPM) "repels 10 million attempted digital intrusions per month,"[305] but it failed to catch a massive hack that transferred millions of federal employee records to a foreign entity.[306] These records apparently included fingerprints and background checks on individuals seeking security clearance.[307] The government had not protected the OPM database with two-factor authentication, and a government security contractor with access to the OPM database had its security credentials stolen, permitting access to the database.[308] While the U.S. government did not attribute the strike to any foreign actor, others pointed the finger at China.[309]

Second, beginning as early as 2019, the Russian Foreign Intelligence Service infiltrated SolarWinds, a Texas company that provided network monitoring and device management software to the federal government.[310] Russia did not need any company ownership to engineer this hack of SolarWinds. By infiltrating SolarWinds's monitoring software, the foreign actor injected its surveillance software into the networks of the U.S. Department of Defense, Department of Homeland Security, and the Treasury Department, as well as several government contractors.[311] Microsoft's President Brad Smith described it as "the largest and most sophisticated attack the world has ever seen."[312]

The third hack is perhaps the most consequential. From 2015 to 2016, Russian hacking crews nicknamed Fancy Bear and Cozy Bear obtained emails from the Hillary Clinton campaign using an old-fashioned phishing attack, tricking her campaign manager into entering his login information into the hackers' website.[313] Again, the hackers did not rely on ownership or control over the

305. Brendan I. Koerner, *Inside the Cyberattack That Shocked the US Government*, WIRED (Oct. 23, 2016, at 17:00 ET), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government.

306. *In re* U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 49 (D.C. Cir. 2019) ("In 2014, cyberattackers breached multiple U.S. Office of Personnel Management ('OPM') databases and allegedly stole the sensitive personal information—including birth dates, Social Security numbers, addresses, and even fingerprint records—of a staggering number of past, present, and prospective government workers. All told, the data breaches affected more than twenty-one million people.").

307. Josh Fruhlinger, *The OPM Hack Explained: Bad Security Practices Meet China's Captain America*, CSOONLINE (Feb. 12, 2020), https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html [https://perma.cc/E537-KKYU].

308. *Id.*; *In re* U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d at 50, 52.

309. Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 548–49 (2020).

310. U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-104746, FEDERAL RESPONSE TO SOLARWINDS AND MICROSOFT EXCHANGE INCIDENTS 13–14 (2022).

311. Kim Zetter, *The Untold Story of the Boldest Supply-Chain Hack Ever*, WIRED (May 2, 2023, at 06:00 EST), https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever.

312. Laurens Cerulus, *SolarWinds is 'Largest' Cyberattack Ever, Microsoft President Says*, POLITICO (Feb. 15, 2021, at 11:56 CET), https://www.politico.eu/article/solarwinds-largest-cyberattack-ever-microsoft-president-brad-smith [https://perma.cc/2GTL-V8LG].

313. *See generally* SCOTT J. SHAPIRO, FANCY BEAR GOES PHISHING: THE DARK HISTORY OF THE INFORMATION AGE, IN FIVE EXTRAORDINARY HACKS (2023); *Death by Leaks: Russian Hacking Helped Sink Clinton 2016 Campaign*, FRANCE 24 (July 13, 2018, 22:28 ET), https://www.france24.com/en/20180713-death-leaks-russian-hacking-helped-sink-clinton-2016-campaign [https://perma.cc/Y2NB-5ZPN]; Ellen Nakashima & Shane Harris, *How the Russians Hacked the DNC and Passed Its Emails to WikiLeaks*, WASH. POST (July 13, 2018, at 19:26 ET), https://www.washingtonpost.com/world/national-

corporations providing services, but rather infiltration using social engineering and other hacking techniques.[314]

To engage in hacking, governments no longer need substantial cybersecurity capacity of their own, because they can buy zero-day exploits from commercial surveillance vendors, who sell spying-as-a-service.[315] These vendors are often based in countries that are political allies of the United States.[316] As a Google Threat Analysis Group report finds, "The government customer selects the target, crafts the campaigns that deliver the spyware, then monitors and commands the spyware implant to collect and receive data from the device."[317]

A second common tool for obtaining information is spying. In 2022, a Twitter employee was convicted and sentenced to prison in the United States for spying on behalf of Saudi Arabia.[318] The government charged that he divulged the personal user information of dissidents.[319] Peiter "Mudge" Zatko, Twitter's former

security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html. In the 2016 U.S. Presidential election, the Russian Internet Research Agency used other techniques to promote its divisive agenda via platforms such as Facebook. *See* RENEE DIRESTA ET AL., NEW KNOWLEDGE, THE TACTICS & TROPES OF THE INTERNET RESEARCH AGENCY 4, 99 (2019) https://digitalcommons.unl.edu/senatedocs/2 [https://perma.cc/LF44-6D8F] (upon request from the U.S. Senate Select Committee on Intelligence). Russia did not need to own Facebook to own Facebook. Indeed, information operations proliferate across the many platforms; responsible platforms have teams designed to identify and remove what Meta calls "Coordinated Inauthentic Behavior." *Inauthentic Behavior*, META, https://transparency.meta.com/policies/community-standards/inauthentic-behavior [https://perma.cc/VT3T-XY6U] (last visited Dec. 31, 2025).

314. A massive hack of AT&T cellular records disclosed in July 2024 presents an example of other hacking techniques, as it seems to have utilized vulnerabilities in a U.S.-based cloud security provider. *See* Steve Zurier, *Massive AT&T Breach Linked to Cloud IT Service Provider Snowflake*, SC MEDIA (July 12, 2024), https://www.scmagazine.com/news/massive-att-breach-linked-to-cloud-it-service-provider-snowflake [https://perma.cc/QY7B-M3D4]; Joseph Menn & Aaron Gregg, *AT&T Says Hacker Stole Call Records of 'Nearly All' Wireless Customers*, WASH. POST (July 12, 2024), https://www.washingtonpost.com/business/2024/07/12/att-wireless-hacker-data-breach.

315. *See* WINNONA DESOMBRE BERNSEN, CYBER STATECRAFT INITIATIVE, ATLANTIC COUNCIL, CRASH (EXPLOIT) AND BURN: SECURING THE OFFENSIVE CYBER SUPPLY CHAIN TO COUNTER CHINA IN CYBERSPACE 3–4 (2025), https://www.atlanticcouncil.org/wp-content/uploads/2025/06/Crash-exploit-and-burn_DeSombre-Bernsen.pdf [https://perma.cc/Y4AB-WQJK] (describing markets for zero-days available to Chinese and U.S. governments). Zero-days are software vulnerabilities not yet known to the software vendor. *Id.* at 3.

316. *See, e.g.*, THREAT ANALYSIS GROUP, GOOGLE, BUYING SPYING: INSIGHTS INTO COMMERCIAL SURVEILLANCE VENDORS 22–26 (2024) (identifying commercial surveillance vendors from Greece, Israel, Italy, and Spain); Issie Lapowsky, *Meta Calls on the EU to Step Up Fight Against Spyware*, FAST CO. (Feb. 14, 2024), https://www.fastcompany.com/91028657/meta-calls-on-the-eu-to-step-up-the-fight-against-spyware [https://perma.cc/E2LT-NM8D] ("Meta is ramping up pressure on European officials to crack down on the burgeoning commercial spyware industry, after the company announced it had disrupted a number of Italian and Spanish firms that were advertising their surveillance services in plain sight.").

317. THREAT ANALYSIS GROUP, *supra* note 316, at 19.

318. *See* Kevin Collier, *Former Twitter Employee Sentenced to More Than Three Years in Prison for Spying for Saudi Arabia*, NBC NEWS (Dec. 14, 2022, at 17:13 EST), https://www.nbcnews.com/tech/security/former-twitter-employee-sentenced-three-years-prison-spying-saudi-arab-rcna61384 [https://perma.cc/LE9K-LSJJ].

319. Kalley Huang & Kate Conger, *Former Twitter Employee Convicted of Charges Related to Spying for Saudis*, N.Y. TIMES (Aug. 9, 2022), https://www.nytimes.com/2022/08/09/technology/twitter-saudi-arabia-spying-ahmad-abouammo.html.

head of security, filed a whistleblower complaint with the Securities and Exchange Commission and the Federal Trade Commission in 2022, alleging that a foreign country had pressured Twitter to hire employees chosen by that government.[320] In 2024, federal authorities arrested a Chinese national who worked for Google in California for allegedly stealing AI trade secrets to share with a Chinese firm.[321]

Finally, the vast collection of personal data by online companies yields yet another avenue for foreign government access to data: buying the data from brokers. For example, reporters recently purchased data that allowed them to track soldiers and contractors at a U.S. airbase in Germany, from their homes to air force bases to brothels.[322] As one scholar notes, "there is certainly nothing stopping the Chinese government, or any other foreign government for that matter, from buying Americans' data through data brokers."[323] An Executive Order issued in February 2024 sought to ban some of those sales via data brokers.[324] Congress then adopted similar provisions in the Protecting Americans' Data from Foreign Adversaries Act, part of the omnibus bill that also enacted the TikTok law.[325] The Data Security Program now prohibits data brokerage transactions involving countries of concern and covered persons, and defines data brokerage fairly broadly, encompassing:

> [T]he sale of data, licensing of access to data, or similar commercial transactions . . . involving the transfer of data from any person (the provider) to any other person (the recipient), where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.[326]

Thus, there are multiple alternatives to exfiltrating data—hacking, spying, and buying data—that do not depend on ownership or control of components of the supply chain. Exfiltration of data, after all, does not depend on physical control. Rather than targeting ownership, a cybersecurity review should target information

320. *See* Joseph Menn, Elizabeth Dwoskin & Cat Zakrzewski, *Former Security Chief Claims Twitter Buried 'Egregious Deficiencies'*, WASH. POST (Aug. 23, 2022, at 12:27 EST), https://www.washingtonpost.com/technology/interactive/2022/twitter-whistleblower-sec-spam.

321. Glenn Thrush & Nico Grant, *Ex-Google Engineer Charged with Stealing A.I. Secrets for Chinese Firm*, N.Y. TIMES (Mar. 6, 2024), https://www.nytimes.com/2024/03/06/us/politics/google-engineer-china-ai-theft.html.

322. Dhruv Mehrotra & Dell Cameron, *Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany*, WIRED (Nov. 19, 2024, at 23:00 ET), https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany ("In February of 2024, reporters from BR and Netzpolitik.org obtained a free sample of this kind of data from Datastream Group, a Florida-based data broker. The dataset contains 3.6 billion coordinates—some recorded at millisecond intervals—from up to 11 million mobile advertising IDs in Germany over what the company says is a 59-day span from October through December 2023.").

323. Faison, *supra* note 86, at 130.

324. *See* Exec. Order No. 14117, 89 Fed. Reg. 15421, 15423 (Mar. 1, 2024).

325. *See* 15 U.S.C § 9901(a).

326. 28 C.F.R. § 202.214 (2025).

collection, processing, access, and sharing. Rather than focusing largely on who owns a service provider, risk assessments should examine how data moves, how it is stored, and how it is accessed and shared. Cybersecurity guidance from the U.S. General Services Administration examines ownership alongside key questions such as access protocols, vendor practices, and insider threat controls.[327]

B. REDUCES COMPETITION

Requirements of immunity from foreign jurisdiction or other national firewalls necessarily reduce competition in information services. By limiting potential providers to only those without a presence in a disfavored state, immunity from foreign jurisdiction dramatically narrows the available service providers. This loss of choice harms companies across the economy because they now have fewer providers, which are likely to be able to charge higher prices while providing worse service.[328] Ironically, Digital Walls can also undermine cybersecurity; local suppliers may not have the same cybersecurity protections as their global competitors.[329]

In recognition of the costs, China has retreated somewhat from the strict approach towards cross-border data flows, largely because of concern that curtailing data flows from China will harm its own economy.[330] Where the earlier rules had indicated that "important data" could not be exported, without defining important terms, the Cyberspace Administration of China has recently signaled that data can flow out, unless it has been designated as important.[331]

C. EXPENSIVE

Beyond the higher costs resulting from reduced competition, national firewalls are expensive to maintain. They require public resources for enforcement.[332] Companies must expend resources to seek to comply. TikTok, for example, has spent one-and-a-half billion dollars to implement the restructuring needed to

---

327. *See* GEN. SERVS. ADMIN., CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) ACQUISITION GUIDE 5–8 (2025).

328. *See* Chander & Lê, *supra* note 12, at 721 (explaining that "data localization raises costs for local businesses, reduces access to global services for consumers, hampers local start-ups, and interferes with the use of the latest technological advances").

329. *See id.* at 719 ("[T]he Protected Local Provider offering storage and processing services may be more likely to have weak security infrastructure than companies that continuously improve their security to respond to the ever-growing sophistication of cyberthieves.").

330. Stuart Lau, *Deal over Dim Sum: China Caves to EU on Data to Keep Investors Sweet*, POLITICO (Nov. 9, 2023, at 05:10 CET), https://www.politico.eu/article/deal-over-dim-sum-china-caves-eu-data-keep-investors-sweet [https://perma.cc/ZX9M-7U7K].

331. Tom Hancock, *China Loosens Cross-Border Data Rules to Ease Business Pressure*, BLOOMBERG (Mar. 23, 2024, at 21:07 ET), https://www.bloomberg.com/news/articles/2024-03-22/china-loosens-cross-border-data-rules-to-ease-business-pressure.

332. National firewalls require significantly higher costs compared to the cost of more traditional cybersecurity firewalls to protect specific computers. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-16-294, INFORMATION SECURITY: DHS NEEDS TO ENHANCE CAPABILITIES, IMPROVE PLANNING, AND SUPPORT GREATER ADOPTION OF ITS NATIONAL CYBERSECURITY PROTECTION SYSTEM 12, 16, 24–25 (2016) (stating that the U.S. government's firewall, known as the Einstein program, cost $5.7 billion dollars to develop, yet it is still only "partially . . . meeting its stated system objectives").

comply with U.S. national security demands, and is planning to spend twelve billion euros to comply with European user data protection requirements as well.[333]

D. INVITES RETALIATION

Firewalls beget firewalls. Restrictions that strike at foreign providers will often be met with retaliation from the home countries of those providers.[334] It is true that, until recently, the United States did not respond to the Great Firewall of China by shutting out Chinese apps. But for the first two decades, the United States did not face the prospect of any wildly popular Chinese internet services in the United States. There simply were not any Chinese major information apps to kick out. Beginning with TikTok, and extending to consumer retailers Shein and Temu, the United States has finally begun to grapple with Chinese companies that are finding success on our shores.[335]

Furthermore, even if China has already banned U.S.-based information services such as Facebook, *The New York Times*, and Wikipedia,[336] it has plenty of other possible targets if it chooses to retaliate for U.S. bans of its apps. Indeed, in a "tit-for-tat" move in the wake of U.S. executive orders targeting TikTok and WeChat, China established an "unreliable entity list" in September 2020.[337] When the *Wall Street Journal* reported that the Chinese government may be banning government employees from bringing iPhones to government offices, Apple saw nearly a *two hundred billion dollar* decline in its market capitalization.[338]

With respect to the argument that turnabout is fair play, Justice Brennan offered a sharp riposte: "That the governments which originate this propaganda

---

333. *See* Kristen Cabrera & Sean Saldana, *Project Texas: Inside TikTok's Billion-Dollar Plan to Stay in America*, TEX. STANDARD (Mar. 27, 2023, at 15:59 EST), https://www.texasstandard.org/stories/project-texas-tiktok-plan-stay-america-oracle-security [https://perma.cc/85F7-R86Z]; Theo Bertram, *TikTok Sets New Standards for Security and Sustainability Through €12bn Project Clover Programme*, TIKTOK: NEWSROOM (Nov. 30, 2023), https://newsroom.tiktok.com/en-eu/tiktok-sets-new-standards-for-security-and-sustainability-through-12-bn-project-clover-programme [https://perma.cc/VT3E-EANM].

334. *See* Tim Wu, *A TikTok Ban Is Overdue*, N.Y. TIMES (Aug. 18, 2020), https://www.nytimes.com/2020/08/18/opinion/tiktok-wechat-ban-trump.html ("[T]he threatened bans on TikTok and WeChat, whatever their motivations, can also be seen as an overdue response, a tit for tat, in a long battle for the soul of the internet."); Lemley, *supra* note 3, at 1413.

335. *See* Lemley, *supra* note 3, at 1407; Ryan McMorrow & William Langley, *Chinese Fast-Fashion Rivals Temu and Shein Take 'War' for US to Court*, FIN. TIMES (July 19, 2023), https://www.ft.com/content/c1ff4f17-03ed-408b-8cb7-07a429d6399d.

336. *See* Li Yuan, *A Generation Grows Up in China Without Google, Facebook or Twitter*, N.Y. TIMES (Aug. 6, 2018), https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html.

337. Bu, *supra* note 273, at 159.

338. *See* Nicole Goodkind, *Apple Lost $200 Billion in Two Days After Reports of iPhone Ban in China*, CNN (Sep. 7, 2023, at 16:29 EDT), https://www.cnn.com/2023/09/07/investing/apple-stock-iphone-china-ban [https://perma.cc/U5SU-LXBM]; Kubota, *supra* note 253; Dan Gallagher, *Apple Becomes the Biggest U.S.-China Pawn Yet*, WALL ST. J. (Sep. 8, 2023, at 00:01 ET), https://www.wsj.com/tech/apple-becomes-the-biggest-u-s-china-pawn-yet-ad093256 (describing reports of the Chinese government ban as "costing the company about $194 billion in market value"). The Chinese government denied the reports. *See* Rachel Liang, *China Says No Laws, Regulations Banning Use of Apple's iPhones*, WALL ST. J. (Sep. 13, 2023, at 05:51 ET), https://www.wsj.com/tech/china-denies-ban-on-apples-iphones-aca9f2af.

themselves have no equivalent [First Amendment] guarantees only highlights the cherished values of our constitutional framework; it can never justify emulating the practice of restrictive régimes in the name of expediency."[339]

E. HIGHLY INTRUSIVE

Controlling cross-border data flows will require an enormous amount of surveillance. In addition to apps and other information services, this will require assessing the many modern devices that connect to the internet to provide smart services. In order to determine whether a company might jeopardize personal data, one needs to inquire into decision-making at all levels—from the corporate bosses to the line employees. After all, bosses may order data to be disclosed (risking whistleblower actions), but employees may transfer data without such an order. Taken to its logical conclusion, immunity from foreign jurisdiction would also mean that the local company cannot employ anyone who is a citizen of the foreign country if that person might gain access to personal data. When a Dutch ministry sought advice from a U.S. law firm about risks of U.S. intelligence services gaining access to that country's citizens' data, the law firm recommended: "[I]t is advisable not to employ US nationals who have access to relevant data."[340] Of course, just as corporate ownership or incorporation is not enough to determine the risks of foreign compulsion, even citizenship is not enough to determine whether the individual might be susceptible to foreign pressure or hold foreign allegiance.[341] One would have to understand each employee's history and personal relationships to understand the risks they entailed. Perhaps every employee in such companies would have to go through a national security clearance, repeated at appropriate intervals.

The logic of such loyalty checks means ultimately vetting the major shareholders of corporations to see whether they present a security risk. Every vendor to those companies would need to be vetted if the vendor might have access to those companies' data. And then every vendor's manager, employee and shareholder would also need to be vetted. And the same for the vendors' vendors, ad absurdum.

F. INCREASES GOVERNMENT CONTROL

The power to select who can and cannot provide services that include personal data can be employed for political ends. A government could use such power to declare a service with foreign connections off limits when that service is not bending to the government's political demands. Governments might, for example, target such services when those services permit criticism of the government

339. Lamont v. Postmaster Gen., 381 U.S. 301, 310 (1965) (Brennan, J., concurring).

340. Memorandum from Gretchen Ramos, Andrea Maciejewski & Herald Jongen, Greenberg Traurig LLP on Application of the CLOUD Act to EU Entities to Dutch Ministry of Just. & Sec. (July 26, 2022) (on file with author).

341. Gordon Hirabayashi, Mitsuye Endo, and Fred Korematsu were all U.S. citizens, but were nevertheless interned during World War II. *See* Hirabayashi v. United States, 320 U.S. 81, 83 (1943); *Ex parte* Mitsuye Endo, 323 U.S. 283, 284–85 (1944); Korematsu v. United States, 323 U.S. 214, 215–16 (1944).

beyond that which the government is willing to tolerate.[342] National security, or freedom from foreign surveillance, can disguise governmental actions taken for other reasons.[343]

To establish the threat that TikTok posed to U.S. national security, the U.S. government pointed to Chinese government "authority and supervision over nominally private . . . organizations";[344] Chinese laws that require private persons to assist Chinese intelligence services;[345] and Chinese rules that give the government the power to "take control of an organization's facilities, which includes communications equipment."[346] The U.S. government was also worried that the Chinese government might compel TikTok to push Chinese Communist propaganda to U.S. residents.[347] These are, of course, serious concerns; J. Benton Heath, for example, includes "malicious cyber-enabled activities" among his list of concerns reflected in the "new national security agenda."[348] China's National Intelligence Law requires "[a]ll organizations and citizens [to] . . . assist . . . national intelligence efforts in accordance with law."[349] The following provision conditions this support: "National intelligence efforts shall be conducted in accordance with law, shall respect and protect human rights, and shall preserve the lawful rights and interests of individuals and organizations."[350] There are

342. *See, e.g.*, David McCabe, *TikTok Bid Highlights Oracle's Public Embrace of Trump*, N.Y. TIMES (Sep. 4, 2020), https://www.nytimes.com/2020/09/04/technology/oracle-tiktok-trump.html (noting that, "as [Oracle] tries to buy the U.S. operations of TikTok . . . its embrace of the [Trump] administration could be helpful").

343. *See, e.g.*, LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 8 (2016) (discussing past intelligence programs of U.S. government agencies and how, "[i]n each case, the initial purpose was to protect against national security threats[,] [b]ut the targets quickly expanded to include petty criminals and anyone with divergent political views").

344. Defendants' Memorandum in Opposition to Plaintiffs' Renewed Motion for a Preliminary Injunction against Commerce Department Prohibitions at 4, TikTok Inc. v. Trump, No. 20-CV-2658, 2020 WL 6883229 (D.D.C. Oct. 23, 2020) [hereinafter Defendants' Memorandum in Opposition] (noting that China exercises supervision over non-governmental organizations "through Party Committees or Corporate CCP Committees at those entities").

345. *Id.* ("[I]n 2017, the PRC enacted the National Intelligence Law, which obliges individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of intelligence work." (internal quotation marks omitted)).

346. *Id.* (citation omitted); *see* Zhonghua Renmin Gongheguo Guojia Qingbao Fa (中华人民共和国国家情报法) [National Intelligence Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., June 27, 2017, amended and effective Apr. 27, 2018), art. 17, 2017 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 474-481, *translated in PRC National Intelligence Law (as Amended in 2018)*, CHINA L. TRANSLATE (June 27, 2017), https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017 [https://perma.cc/3F8D-KZY2].

347. Defendants' Memorandum in Opposition, *supra* note 344, at 3 (describing "[t]he communist government of the People's Republic of China [as] a significant and growing national security threat").

348. *Cf.* Heath, *supra* note 55, at 1036 (internal quotation marks omitted) (quoting Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 15, 2019)).

349. National Intelligence Law of the People's Republic of China, art. 7.

350. *Id.* at art. 8; *see also* Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sep. 1, 2021), art. 35, 2021 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 951-962, *translated in Data Security Law of the People's Republic of China*,

reasonable concerns about the effectiveness of such constraints. These rules apply to "[a]ll organizations," not just domestic ones,[351] indicating that the Chinese government might intend for even major U.S. technology companies to fall within the scope of these rules. Thus, companies as prolific as Apple or Microsoft, or at least their Chinese subsidiaries, must comply with China's National Intelligence Law.[352] In anticipation of U.S. national security concerns, Microsoft is in the process of moving its artificial intelligence engineers out of China.[353]

In response to these concerns, ByteDance and TikTok negotiated with CFIUS to establish mitigation measures to limit the possibility that ByteDance would be forced to commandeer TikTok's data for the Chinese government.[354] Although that mitigation agreement proved insufficient for the U.S. Congress and the Biden Administration,[355] it is instructive to examine the implications of Project Texas for the rights of people in the United States.

Under TikTok's "Project Texas," TikTok, Inc., a California company, was splintered into two companies, the original company, and a new company, TikTok U.S. Data Security (TTUSDS).[356] TTUSDS would be a new business entity, entirely independent of ByteDance, responsible for managing the business functions that either require access to data of U.S. citizens or are responsible for content moderation decisions for U.S. users.[357] Crucially, its board of directors would be approved by the U.S. government.[358] *The Washington Post* reported that "the Chinese company would cede authority over TikTok's U.S. operations

---

NAT'L PEOPLE'S CONG. OF PEOPLE'S REPUBLIC OF CHINA (June 10, 2021), http://en.npc.gov.cn.cdurl.cn/2021-06/10/c_689311_2.htm [https://perma.cc/AGT3-EQYQ] ("Where a public security organ or national security organ needs to obtain data for the sake of national security or for investigating crimes in accordance with the law, strict approval formalities shall be completed in accordance with the relevant provisions of the state and data be obtained in accordance with the law.").

351. National Intelligence Law of the People's Republic of China, art. 7.

352. *See, e.g.*, Erie & Streinz, *supra* note 143, at 33 (noting how "Apple was forced to host Chinese users' iCloud accounts in data centers located in mainland China . . . to comply with the Cybersecurity Law").

353. Raffaele Huang & Yoko Kubota, *Microsoft Asks Hundreds of China-Based AI Staff to Consider Relocating Amid U.S.-China Tensions*, WALL ST. J. (May 16, 2024, at 07:43 ET), https://www.wsj.com/tech/ai/microsoft-asks-hundreds-of-china-based-ai-staff-to-relocate-amid-u-s-china-tensions-b626ff8c.

354. Draft National Security Agreement, §§ 11.5, 11.8–.10.

355. *See* Emily Baker-White, *Trump's TikTok Deal Seems Like a Repackaged Version of the One the Biden White House Rejected*, FORBES (Sep. 29, 2025, at 14:22 EDT), https://www.forbes.com/sites/emilybaker-white/2025/09/29/trumps-tiktok-deal-seems-like-a-repackaged-version-of-the-one-the-biden-white-house-rejected.

356. *See* Matt Perault & Samm Sacks, *Project Texas: The Details of TikTok's Plan to Remain Operational in the United States*, LAWFARE (Jan. 26, 2023, at 08:01 ET), https://www.lawfaremedia.org/article/project-texas-the-details-of-tiktok-s-plan-to-remain-operational-in-the-united-states [https://perma.cc/GWT7-5SAP]; Draft National Security Agreement, § 2.1.

357. *See* Perault & Sacks, *supra* note 356; Draft National Security Agreement § 2.7 ("ByteDance shall not play any role in or make any attempt to influence, determine, direct, or decide the operations, management, or leadership of TTUSDS."); *see also* Draft National Security Agreement, §§ 2.1–3.11 (describing the formation and governance of TTUSDS).

358. Draft National Security Agreement, §§ 3.1–3.2.

to a three-person board whose members CFIUS would essentially select."[359] Under the draft agreement, U.S. government agencies like the DOJ or the DOD would have the authority to "[e]xamine TikTok's U.S. facilities, records, equipment and servers with minimal or no notice."[360] TikTok would have to comply with "Lawful U.S. Process," defined as "U.S. federal, state, or local orders or authorizations, and other orders or legal process, statutory authorizations, or certifications from U.S. federal, state, or local law enforcement officials for Access to or disclosure of information, user communications, or content."[361] TikTok would have to report changes to its source code and content moderation systems to government agencies, and the agencies could demand that ByteDance "promptly alter" its source code to "ensure compliance" at any time.[362] In the negotiation with CFIUS, ByteDance and TikTok sought to modify the agreement to prevent the U.S. government "from demanding changes to TikTok's recommendation algorithm simply because it recommended content that the government does not like."[363] This account of the negotiations reveals the rather unlikely spectacle of a Chinese-owned company negotiating to protect the civil liberties of U.S. residents against the U.S. government.

Furthermore, replacing foreign companies with domestic ones offers increased opportunities for public corruption when Executive Branch officials have a role in selecting who can stay and who must leave.[364] In the absence of clear and constrained standards, regulatory discretion can be influenced by political loyalty, lobbying efforts, or personal gain rather than security concerns, potentially opening the door to a "pay-to-play" regulatory compliance regime where politically connected companies are favored while others are excluded.[365]

---

359. Drew Harwell, *TikTok and U.S. Rekindle Negotiations, Boosting App's Hopes for Survival*, WASH. POST (Sep. 15, 2023, at 07:00 EDT), https://www.washingtonpost.com/technology/2023/09/15/tiktok-ban-us-negotiations.

360. Emily Baker-White, *A Draft of TikTok's Plan to Avoid a Ban Gives the U.S. Government Unprecedent Oversight Power*, FORBES (Apr. 15, 2025, at 16:55 EDT), https://www.forbes.com/sites/emilybaker-white/2023/08/21/draft-tiktok-cfius-agreement; *see* Draft National Security Agreement, §§ 17.1–17.2.

361. Draft National Security Agreement, §§ 1.15, 7.1.

362. *Id.* at § 9.15 (giving U.S. government the ability to demand that ByteDance "promptly alter the Source Code . . . to ensure compliance with this Agreement"); *see also* Harwell, *supra* note 359 (noting the National Security Agreement's terms on source code and compliance); Draft National Security Agreement § 9.13 (giving U.S. government the ability to demand that ByteDance "promptly implement any necessary changes or updates to the Software implementing the . . . Content Moderation Process").

363. Baker-White, *supra* note 360.

364. *See* OECD, STATE-OWNED ENTERPRISES AND CORRUPTION: WHAT ARE THE RISKS AND WHAT CAN BE DONE? (2018), https://www.oecd.org/en/publications/state-owned-enterprises-and-corruption_9789264303058-en/full-report.html (discussing how state-owned enterprises are particularly vulnerable to corruption due to the discretion afforded to government officials, political influence in decisionmaking, and weak corporate governance structures); *cf.* Ana Swanson & Lauren Hirsch, *'Golden Share' in U.S. Steel Gives Trump Extraordinary Control*, N.Y. TIMES (June 15, 2025), https://www.nytimes.com/2025/06/15/us/politics/golden-share-us-steel-nippon-trump.html (noting how the unusual "golden share" arrangement in Japan's Nippon Steel acquisition of U.S. Steel would give President Trump enormous influence over and a permanent stake in U.S. Steel).

365. Empirical studies of procurement and state-owned enterprises show that discretionary decisionmaking of this kind increases corruption risks, distorts markets, and undermines the stated policy objectives of national security or economic efficiency. *See, e.g.*, OECD, *supra* note 364, at 20

To conclude, in an irony that must not have been lost on the U.S. and TikTok negotiators, Project Texas gave the U.S. government many of the excessive governmental powers that it has criticized China for embracing.[366] These include government supervision of private parties and government authority to commandeer the company's equipment and data.[367] As Karim Farhat observes, "Project Texas puts the U.S. government in direct control of a media outlet's data and asserts a blanket right to review and censor its algorithms and content."[368] The TikTok Law similarly gave the President enormous powers to decide who could own a massive speech platform in the United States.

* * *

In sum, Digital Walls prove weak—easily scalable, expensive to maintain, and harmful to one's own businesses and citizens. They come at high costs and offer only limited benefits.

IV. CORPORATE RESPONSES: DIGITAL SWITZERLANDS

Corporations are increasingly taking steps to assure host countries that those corporations will not become the eyes and ears of their home country. Corporations, for example, can minimize data collection and retention so that there is less data vulnerable to foreign surveillance; they can encrypt data to make it more difficult to access; they can store and process data in jurisdictions that pose fewer risks; they can localize data in the host country; they can reincorporate in neutral jurisdictions; they can employ local trustees to distance their own control over the data; and they can challenge excessive governmental requests for information through the legal system. Through such techniques, corporations hope to be seen as "Digital Switzerlands"—neutral among the various governments of the countries in which they operate—rather than extensions of their home state.[369]

(noting that 49% of the 213 state-owned companies surveyed reported at least one corrupt act, and identifying the top three risks as "(i) violations of data protection and privacy; (ii) favouritism . . . and (iii) non-declaration of conflict of interest"); Marly Tatiana Celis Galvez, Vitezslav Titl & Fredo Schotanus, *Discretion and Political Favoritism: Evidence from Two Reforms in Public Procurement*, 91 S. ECON. J. 915, 916 (2024) ("Increasing [bureaucratic] discretion, even in difficult times, carries risks of inefficiency and corruption.").

366. *See* Harwell, *supra* note 359 (noting that Project Texas "would raise the risk that the government could subtly shape what TikTok users see—similar to what the app's critics have warned of regarding influence from the Chinese state").

367. Defendants' Memorandum in Opposition, *supra* note 344, at 4.

368. Karim Farhat, *TikTok's Project Texas: The Wrong Template for Tomorrow's Digital Economy*, GA. TECH: SCH. OF PUB. POL'Y: INTERNET GOVERNANCE PROJECT (Mar. 9, 2023), https://www.internetgovernance.org/2023/03/09/tiktoks-project-texas-the-wrong-template-for-tomorrows-digital-economy [https://perma.cc/JFP7-P3FF] (comparing China's 2017 Cybersecurity Law and its 2021 Data Security Law with Project Texas, and finding that Project Texas "gives the government the power to harass a publisher if it releases content that is deemed politically controversial").

369. Kristen Eichensehr elaborated the concept of "Digital Switzerlands," borrowing a term offered by Microsoft President Brad Smith in 2017. *See* Eichensehr, *supra* note 69, at 665–66. She uses the term to describe "the companies' role in the digital ecosystem and in international affairs," focusing in particular on the ways that companies seek to counter government demands for information. *Id.* at 667.

This Part begins by surveying and cataloging various "Digital Switzerland" measures that companies are taking. Yet, another measure is possible: exit. Companies can simply give up a market, recognizing that the risks of operating in that market do not justify the benefits. The last Section discusses the inherent limitations of Digital Switzerland measures.

A. DATA MINIMIZATION AND ENCRYPTION

One method to reduce the threat of data access by governments is simply to collect less data. Data minimization, accordingly, is a key part of the corporate toolkit to avoid governmental data compulsion actions. Another mechanism is encryption, where data held by a company is encrypted to prevent access without the decryption key. For example, Apple began encrypting iPhones by default after the Edward Snowden revelations.[370]

B. DATA LOCALIZATION

Perhaps the most popular way to appease local authorities is to localize data.[371] Alibaba, for example, built servers in Vietnam to help companies comply with Vietnamese data localization obligations.[372] Faced with similar Vietnamese demands, Meta sought to placate authorities by meeting their demands to censor content instead.[373] For its part, Microsoft has offered European localization within what it calls the "EU Data Boundary."[374]

Perhaps the most extensive effort to reduce risks of foreign surveillance or manipulation was the plan offered by TikTok in the United States discussed in Part IV.F above. TikTok's plan combined data localization, a local data trustee, local reincorporation, and additional steps.[375] Private data of U.S. persons would be stored only on Oracle's servers in the United States.[376] TikTok's software,

---

My account expands the concept of a "Digital Switzerland" by identifying additional strategies for neutrality that corporations are taking.

370. Kevin Poulsen, *Apple's iPhone Encryption Is a Godsend, Even if Cops Hate It*, WIRED (Oct. 8, 2014, at 06:30 ET), https://www.wired.com/2014/10/golden-key [https://perma.cc/ZA5N-S77Q].

371. *See, e.g.*, Chander & Lê, *supra* note 12, at 679, 721 (explaining that "data localization measures are often motivated, whether explicitly or not, by desires to promote local economic development"); Wenxi Lu, Note, *Data Localization: From China and Beyond*, 31 IND. J. GLOB. LEGAL STUD. 183, 193 (2024) (noting the "global trend of data sovereignty, which means more and more countries have embraced the idea that online data and information are subject to domestic jurisdiction").

372. *See* Lien Hoang, *Alibaba to Build Vietnam Data Center to Follow Local Storage Law*, NIKKEI: ASIA (May 1, 2024, at 10:34 JST), https://asia.nikkei.com/Business/Technology/Alibaba-to-build-Vietnam-data-center-to-follow-local-storage-law.

373. *See* Rebecca Tan, *Facebook Helped Bring Free Speech to Vietnam. Now It's Helping Stifle It.*, WASH. POST (June 19, 2023, at 02:00 EST), https://www.washingtonpost.com/world/2023/06/19/facebook-meta-vietnam-government-censorship.

374. Brad Smith, *Answering Europe's Call: Storing and Processing EU Data in the EU*, MICROSOFT: EU POL'Y BLOG (May 6, 2021), https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary [https://perma.cc/7JHV-JHZ8]; *see What Is the EU Data Boundary?*, MICROSOFT (Feb. 26, 2024), https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn [https://perma.cc/8ARY-5JNV].

375. *See supra* notes 344–68 and accompanying text.

376. *See* Draft National Security Agreement § 8.5 ("[TikTok U.S. Data Security] shall ensure that all such [content delivery network] servers utilized for the delivery of content in the United States reside exclusively in the United States."); *id.* at § 11.5 ("The Transaction Parties shall ensure that all Protected

including its recommendation algorithm, would be deployed through Oracle's infrastructure and reviewed by Oracle and another CFIUS-approved third party.[377] TikTok's content moderation—both human and algorithmic—would be subject to third-party verification and monitoring.[378] The new company's officers would have "strong credentials in national security" and would be "Resident Sole U.S. Citizens."[379] They would "have, or [be] eligible for, a U.S. personnel security clearance"[380]—thus ensuring that, in practice, they would be former U.S. government officials or vetted government contractors. The U.S. government would even hold a "kill switch," able to shut off the app if TikTok violated its national security commitments.[381] Despite these extensive commitments, ByteDance and TikTok failed to satisfy the U.S. government that it would be safe for TikTok to continue to operate in the United States under ByteDance's ownership.

C. DATA TRUSTEES

Another strategy companies employ in order to assuage fears of foreign influence is to locate a trusted local partner, through which they continue to offer services. In 2015, for example, seeking to respond to German concerns about U.S. surveillance of German residents' data in the wake of the Snowden revelations, Microsoft offered an innovative "data trustee" arrangement as an option for clients in that country.[382] Various Microsoft cloud services would be offered by computer servers owned and operated by the German telecommunications giant Deutsche Telekom.[383] A Deutsche Telekom unit would control access to customer data, and Microsoft could not access customer data without approval from and supervision by the German data trustee or customer.[384] Although the two companies dissolved their partnership in 2018 due to a combination of high prices

Data . . . is stored and remains . . . exclusively in the United States, with no transmittal outside of the United States.").

377. *Id.* at § 9.13.

378. *Id.* at §§ 5.4, 9.13, 16.6.

379. *Id.* at § 3.1. "Resident Sole U.S. Citizens" are citizens of the United States who reside in the United States and who do not hold another citizenship. *See id.* § 1.25.

380. *Id.* at § 3.1.

381. *See id.* at §§ 21.3, 21.5 (providing that failure to comply with the Draft National Security Agreement can result in a "Temporary Stop," preventing users from accessing the TikTok Platform, or, if a Temporary Stop is not fully implemented, a "Suspension of Service").

382. *T-Systems to Act as Data Trustee for Microsoft Cloud in Germany*, DIGITALISATION WORLD, https://digitalisationworld.com/news/46236/t-systems-to-act-as-data-trustee-for-microsoft-cloud-in-germany [https://perma.cc/UZK5-5FZA] (last visited Dec. 31, 2025); *see also* Cerulus & von der Burchard, *supra* note 190 ("Snowden's revelations have led to major arguments over the security and privacy of Europeans.").

383. *See T-Systems to Act as Data Trustee for Microsoft Cloud in Germany*, *supra* note 382; *Deutsche Telekom to Act as Data Trustee for Microsoft Cloud in Germany*, DEUTSCHE TELEKOM AG (Nov. 11, 2015), https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-to-act-as-data-trustee-for-microsoft-cloud-in-germany-362074 [https://perma.cc/W8KM-ZZ8F].

384. *See T-Systems to Act as Data Trustee for Microsoft Cloud in Germany*, *supra* note 382.

and issues with stability, performance, and security,[385] newer companies have adopted similar structures. Temu, for example, uses a similar model to store U.S.-persons data on Microsoft servers in the United States.[386]

In China, in response to the Chinese Cybersecurity Law,[387] Apple adopted a model similar to Microsoft's data trustee arrangement, though that model continues through today and is not optional. Capitulating to government pressure, Apple localized its Chinese user data on computer servers run by a state-owned Chinese firm.[388] As a result, "Apple's compromises have made it nearly impossible for the company to stop the Chinese government from gaining access to the emails, photos, documents, contacts and locations of millions of Chinese residents, according to the security experts and Apple engineers."[389] Salesforce, too, now "relies on a local partner to operate some of its products and services there, effectively isolating its China business from its global operations."[390]

D. REINCORPORATION, OR "ANYWHERE-BUT-CHINA"

Recognizing that their national origins might make them unwelcome elsewhere, some companies are reincorporating into neutral jurisdictions. Chinese firms, in particular, must "grapple with a kneejerk presumption from foreign governments of their fealty to the Chinese Communist Party."[391] Some have thus adopted an effort to refashion themselves as from "Anywhere-But-China" (ABC).[392]

Take the example of Shein and Temu. While "born in China," the fast-fashion giant Shein went so far as to deregister its Chinese company and move its headquarters and incorporation to Singapore in 2022 to assuage national security

---

385. Jos Poortvliet, *Microsoft and Telekom No Longer Offer Cloud Storage Under German Jurisdiction*, NEXTCLOUD (Sep. 4, 2018), https://nextcloud.com/blog/microsoft-and-telekom-no-longer-offer-cloud-storage-under-german-jurisdiction [https://perma.cc/9LBG-UFGV].

386. Temu's privacy policy states:

> Data of Temu U.S. users will be stored in cloud service providers in the U.S. As global one-stop shopping destination, Temu may need to engage service providers in other countries and share your personal information with them for purposes such as order fulfillment. We will ensure that all transfers of personal information comply with applicable U.S. legal requirements.

Temu | Privacy Policy, TEMU (Aug. 14, 2025), https://www.temu.com/privacy-and-cookie-policy.html [https://perma.cc/C9J8-TSRB].

387. *See supra* notes 131–37 and accompanying text.

388. Jack Nicas, Raymond Zhong & Daisuke Wakabayashi, *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China*, N.Y. TIMES (June 17, 2021), https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.

389. *Id.*

390. Elaine Yu & Yoko Kubota, *Companies Try New Strategy to Stay in China: Siloing*, WALL ST. J. (June 25, 2023, at 00:01 ET), https://www.wsj.com/articles/companies-try-new-strategy-to-stay-in-china-siloing-61c88721.

391. *Sarah Zheng, Temu and Shein Keep Trying to Shed Their Chinese Roots*, BLOOMBERG (July 16, at 07:05 EDT), https://www.bloomberg.com/news/newsletters/2024-07-16/temu-and-shein-keep-trying-to-shed-their-chinese-roots.

392. Michael Mariani, *Why "China Plus One" Has Become "Anywhere but China"*, Z2DATA (Mar. 13, 2025), https://www.z2data.com/insights/why-china-plus-one-has-become-anywhere-but-china [https://perma.cc/MKG8-55K2].

concerns of the countries in which it operates.[393] Shein's CEO even described the company as "essentially an 'American company,'" a remark that Shein management then worried would raise trouble in China, which remains a critical part of its supply chain.[394] Indeed, the "model of 'de-Chinafying' to gain business success . . . 'raises questions of loyalty to China that some in Beijing find uncomfortable.'"[395] Similarly, Temu, the successful goods e-commerce company, claims that it "was founded in Boston, Massachusetts in 2022," even though it is owned by Chinese e-commerce giant Pinduoduo.[396] The ABC strategy puts these companies in an awkward position, distancing these companies from their home, while still relying on that home jurisdiction for their supply chain and often expertise and engineering.[397]

E. CHALLENGING GOVERNMENT INFORMATION REQUESTS

Recognizing the concerns of their host jurisdictions, companies have sought to demonstrate their independence from their home jurisdiction by challenging information requests from their home governments. In the wake of the Snowden revelations,

> [A] new political economy [emerged] in which telecommunications and technology firms that were explicitly revealed by Snowden to be National Security Agency (NSA) partners, as well as overseas allies that were shown to be NSA targets, have joined privacy advocates in putting pressure on the White House to cut back on certain intelligence-gathering practices.[398]

Such efforts have continued over the decade since.[399]

---

393. *See* Andrew Edgecliffe-Johnson, *Shein's US Push Complicated by Its Chinese Roots*, FIN. TIMES (Nov. 7, 2023), https://www.ft.com/content/bc97ac49-4717-4861-96b8-aa0881651a48; Mercedes Ruehl & Leo Lewis, *Chinese Companies Set Up in Singapore to Hedge Against Geopolitical Risk*, FIN. TIMES (Nov. 29, 2022), https://www.ft.com/content/a0c11e3e-ab72-4b4b-a55c-557191e53938; Ana Swanson, *As Ties to China Turn Toxic, Even Chinese Companies Are Breaking Them*, N.Y. TIMES (June 15, 2023), https://www.nytimes.com/2023/06/15/business/economy/china-business-tiktok-shein.html.

394. James Kynge, Sun Yu & Ryan McMorrow, *Shein Tries to Suppress Chair's Claim That Fashion Retailer Is 'American*,' FIN. TIMES (June 14, 2024), https://www.ft.com/content/6ecb58d1-2582-48ae-8503-773b228da57e.

395. *Id.* (internal quotation marks omitted).

396. McMorrow & Langley, *supra* note 335.

397. This tension can be illustrated by Temu's antitrust lawsuit accusing Shein of "unlawful exclusionary tactics" for allegedly "forcing its Chinese factories to halt manufacturing for Temu in an attempt to maintain market dominance in the US." *Id.*

398. Samuel J. Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 642 (2016) (footnotes omitted).

399. *See, e.g.*, David McCabe, *Google, Facebook and Snap Push for Surveillance Reforms*, AXIOS (May 26, 2017), https://www.axios.com/2017/12/15/google-facebook-and-snap-push-for-surveillance-reforms-1513302588 [https://perma.cc/MX4T-9Q4U] (noting that "Google, Snap, Uber, Facebook, Microsoft and Amazon were among the more than 30 companies and advocacy groups" asking for reforms to the government's surveillance program under Section 702); Donohue, *supra* note 19, at 23; Sam Sabin, *Privacy Leader Calls for Government Surveillance Program Reforms*, AXIOS (Mar. 7, 2023), https://www.axios.com/2023/03/07/pclob-sec-702-congress-reauthorization-fight [https://perma.

Even while acceding to certain national security-based requests for information, U.S. digital enterprises, in particular, have often challenged U.S. government efforts that they believe are excessive. In 2006, for example, Google successfully challenged a U.S. government subpoena of its search records as overbroad.[400] In 2013, Microsoft resisted complying with a U.S. federal warrant issued pursuant to the Stored Communications Act for the contents of an email account likely stored in Ireland, taking its challenge all the way to the Supreme Court.[401] More recently, Twitter unsuccessfully sought to publicly disclose more detailed information about the national security letters it received from the U.S. government.[402]

The most famous such incident was Apple's refusal to cooperate with the Federal Bureau of Investigation's (FBI) demand to help break into the iPhone of those responsible for a horrific terrorist attack in San Bernardino, California.[403] Unable to unlock the attacker's iPhone due to its security features, the U.S. government obtained a court order under the All Writs Act of 1789 to require Apple to modify its iOS operating system to turn off security features for this particular phone.[404] Apple challenged the order, calling it "the software equivalent of cancer," and arguing that the motion to compel "would make hundreds of millions of customers vulnerable around the world, . . . and also trample civil liberties that are the basic foundation of . . . this country."[405] The issue was resolved when the Department of Justice announced that it had unlocked the iPhone through alternative channels.[406]

---

cc/3C73-R2C4] (discussing continued calls for reform of the government's surveillance power under Section 702).

400. *See* Gonzales v. Google, Inc., 234 F.R.D. 674, 679, 688 (N.D. Cal. 2006) ("The subpoena . . . required the companies to produce the text of users' search queries."). This case also demonstrates that companies will make different calculations at different times; as the court noted in *Gonzales v. Google*, other companies that received the same subpoena seemed to comply. *See id.* at 679 ("AOL, Yahoo, and Microsoft appear to be producing data pursuant to the Government's request.").

401. *See* United States v. Microsoft Corp., 583 U.S. 931 (2017), *vacated as moot*, 584 U.S. 236 (2018).

402. *See* Twitter v. Garland, 61 F.4th 686, 690 (9th Cir. 2023).

403. *See* Todd C. Frankel, *Apple's Tim Cook Calls FBI Request to Crack Terrorist's iPhone 'Bad for America,'* WASH. POST (Feb. 24, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/02/24/apples-tim-cook-calls-fbi-request-to-crack-terrorists-iphone-bad-for-america; Dustin Volz & Mark Hosenball, *FBI Director Says Investigators Unable to Unlock San Bernardino Shooter's Phone Content*, REUTERS (Feb. 9, 2016, at 17:07 EST), https://www.reuters.com/article/us-california-shooting-encryption-idUSKCN0VI22A.

404. *See* Andrew Blankstein, *Judge Forces Apple to Help Unlock San Bernardino Shooter iPhone*, NBC NEWS (Feb. 16, 2016, at 20:00 EST), https://www.nbcnews.com/storyline/san-bernardino-shooting/judge-forces-apple-help-unlock-san-bernardino-shooter-iphone-n519701 [https://perma.cc/62J6-PQJD]; Heather West, *Encryption: It's Not About Good and Bad Guys, It's About All of Us*, CEPA (Dec. 5, 2023), https://cepa.org/comprehensive-reports/encryption-its-not-about-good-and-bad-guys-its-about-all-of-us [https://perma.cc/DYP5-L7T3].

405. Frankel, *supra* note 403.

406. Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html.

Neil Richards and Woodrow Hartzog rightly note that Apple and Microsoft fought these battles with U.S. law enforcement "to earn and keep the trust of their customers."[407] We might go further to note that the companies sought to assure not only their customers, but also foreign governments, as foreign governments, too, were the audience of these efforts.[408] Challenges to U.S. government demands also helped show foreign governments that these U.S.-based entities would, at least at times, go to bat for user privacy even against their home country's law enforcement.

F. LIMITS OF CORPORATE MEASURES

However, corporate efforts can only go so far.

While end-to-end encryption would render information unreadable by even the service provider, it would interfere with any features that require the service system to read the data, including content moderation, fraud detection, search services, and spam filtering.[409] The European Data Protection Supervisor recognized that some "data . . . cannot be effectively pseudonymised or effectively encrypted because the processing requires accessing data in the clear."[410] Encryption and pseudonymization also impacts companies' abilities to collect data to run targeted ads, affecting the profitability of adopting such technologies.[411]

Instead of deploying end-to-end encryption, many companies adopt a model in which they retain the encryption key so that they can perform useful services, such as processing content for features or engaging in targeted advertising.[412] Although this kind of encryption enables user-friendly services, it also makes users more vulnerable to state access.[413] If the company can read the data, it can be compelled to share it.

Data localization and data trustees may not be enough if the local government is not convinced that those measures render the foreign company entirely immune to foreign sovereign demands to produce information. As we have seen, this concern has led to demands for immunity from foreign jurisdiction in the European Union.[414] If the data trustee arrangement leaves the multinational company with the ability to control or access the data, that may render the trusteeship insufficient from the national security perspective. Even TikTok's Project Texas—which went beyond a data trustee model by incorporating an array of commitments including running services exclusively from the data trustee's infrastructure and carefully

407. Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1186 (2017).

408. *See* Frankel, *supra* note 403.

409. *See* Timothy B. Lee, *NSA-Proof Encryption Exists. Why Doesn't Anyone Use It?*, WASH. POST (June 14, 2013), https://www.washingtonpost.com/news/wonk/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it.

410. EUR. DATA PROT. SUPERVISOR, *supra* note 255, at 90.

411. *See* Lee, *supra* note 409.

412. *See id.*

413. *See id.* ("[W]hile this kind of encryption will protect users against ordinary bad guys, it's useless against governments.").

414. *See supra* notes 154–63 and accompanying text.

controlled access to that protected information—failed to satisfy the U.S. Congress or the Biden Administration, resulting in a law requiring either divestiture or ban.[415]

G. EXIT

When efforts to satisfy governments fails, some corporations simply exit. Google left China after hacking attempts and censorship.[416] Albert Hirschman's famous typology—exit, voice, loyalty—describes options for individuals with grievances with organizations.[417] Charles Tiebout analyzed exit from jurisdictions due to the policy environment, specifically the revenue-expenditure pattern.[418] The Tiebout model sees exit as a means of expressing consumer discontent.[419] Both Hirschman and Tiebout focused on exit as a voluntary option, but exit can also be forced upon an individual or a corporation. Host countries can kick out foreign corporations, and home countries can require their corporations to leave a foreign jurisdiction. Corporation exits thus come in three varieties: leaving a country voluntarily, being kicked out, and/or being told by its home government to stay out of a foreign country. We see all varieties of exits here—from corporations like Google leaving a jurisdiction to avoid future entanglements; to the TikTok law compelling TikTok to leave, as long as it is Chinese-owned; to U.S. technology companies being told not to provide their most advanced AI systems in China.[420]

For corporations, like individuals, exit is often a costly option: exit reduces the market for their products, diminishes access to data needed for data analytics and AI training, and lowers opportunities to defray costs through a larger market and benefit from economies of scale.

V. GOVERNMENT RESPONSES

A central impetus for the rise of the national security internet, with border controls for exiting data through mechanisms such as data localization and requirements for immunity from foreign jurisdiction, is concerns over foreign surveillance.[421]

---

415. *See* Exec. Order No. 13942, 85 Fed. Reg. 48637, 48637–38 (Aug. 11, 2020) (IEEPA executive order banning transactions with TikTok); Presidential Order Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51297, 51297 (Aug. 19, 2020) (CFIUS-based executive order requiring divestment); Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, 138 Stat. 955, 955–57 (2024).

416. *See* Miguel Helft & David Barboza, *Google Shuts China Site in Dispute over Censorship*, N.Y. TIMES (Mar. 22, 2010), https://www.nytimes.com/2010/03/23/technology/23google.html.

417. *See generally* ALBERT O. HIRSCHMANN, EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1970).

418. *See* Charles M. Tiebout, *A Pure Theory of Local Expenditures*, 64 J. POL. ECON. 416, 418–19 (1956).

419. *See id.* at 420.

420. *See* Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, 138 Stat. 955 (2024); *supra* notes 284–99. For a discussion of Google's leaving China, see Anupam Chander, *Googling Freedom*, 99 CAL. L. REV. 1 (2011).

421. *See* Barnes & Wong, *supra* note 20. Another possible concern is malware intended to target critical systems. These can be inserted even without ownership of a company—as numerous examples, from the SolarWinds supply chain hack (often attributed to Russia) to Stuxnet (often attributed to the United States and Israel) to WannaCry (attributed by the U.S. to North Korea), and NotPetya (attributed

Unilateral corporate responses may fail to satisfy governments, which may be reluctant to lower their Digital Wall for such measures.

Governments can take steps to build global trust by reducing excessive data gathering, both by the private and the public sector. Rather than erect extensive and problematic border controls to thwart foreign surveillance, countries could agree to limit their own foreign surveillance, thereby diminishing the need for those border controls. Even unilateral steps might build confidence in that country's companies, if broader agreement is harder to achieve.

A. UNILATERAL RESPONSES: LEGAL CONSTRAINTS ON FOREIGN SURVEILLANCE

Governments can take unilateral steps to alleviate the concerns that lead to the national security internet. These include domestic rules governing information, including privacy laws and blocking statutes, and rules limiting their own foreign surveillance activities.

1. Blocking Statutes and Privacy Laws

Countries have enacted blocking statutes or interpreted their laws to make it illegal to share personal data with foreign governments outside officially sanctioned channels. The Electronic Communications Privacy Act includes such a prohibition, as does the Chinese Cybersecurity Law.[422] This is also one way to understand *Schrems II*'s interpretation of European fundamental rights limiting foreign government access to data.[423]

One important method to reduce the risk of personal information falling into the wrong hands is to regulate the collection and processing of personal information, curbing the amount of data that is being collected and the purposes for which

by the U.S. to Russian hackers) demonstrate. *See supra* notes 310–12 and accompanying text; Dina Temple-Raston, *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack*, NPR (Apr. 16, 2021, at 10:05 ET), https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack [https://perma.cc/ZYV7-HFQD]; Spencer Ackerman, *With Stuxnet, Did the U.S. and Israel Create a New Cyberwar Era? [Updated]*, WIRED (Jan. 16, 2011, at 13:58 EST) https://www.wired.com/2011/01/with-stuxnet-did-the-u-s-and-israel-create-a-new-cyberwar-era; *Indicators Associated with WannaCry Ransomware*, DHS: CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (June 7, 2018), https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware [https://perma.cc/G8EP-4J9H]; *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, DOJ: OFF. PUB. AFFS. (Oct. 19, 2020), https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and [https://perma.cc/NHV3-XCTT]. Governments have responded by seeking to make their critical digital infrastructure more secure. *See, e.g.*, Council Directive 2022/2555 of Dec. 14, 2022, Measures for a High Common Level of Cybersecurity Across the Union, amending Regulation (EU) 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, 2022 O.J. (L 333/80) (establishing a new Network and Information Security (NIS2) Directive).

422. *See supra* notes 195–98 and accompanying text.

423. *See supra* notes 159–63 and accompanying text.

it is being processed.[424] As Woodrow Hartzog and Daniel Solove write, "Poor privacy will undermine even the best data security."[425] In particular, "[t]he central privacy principle of data minimization—to collect only data necessary for the purpose at hand and to avoid retaining unnecessary data—can play a key role at minimizing the harmful effects of breaches."[426] Data privacy laws can also help reduce opportunities for employees to exfiltrate data by imposing cybersecurity requirements, duties of care, and internal controls that limit employee access to data and examine whether data is being transferred inappropriately. Furthermore, a comprehensive privacy law reduces both the amount of data for sale by brokers and also the likelihood that brokers can legally sell the data they collect. Unlike Digital Walls, privacy rules can permit foreign companies to supply services as long as they provide appropriate privacy protections for individuals within the jurisdiction.

Of course, it would be foolish to expect foreign intelligence services to simply obey another country's privacy laws, but that is not the point of privacy laws. Privacy laws reduce foreign surveillance by reducing the attack surface—the amount and ubiquity of information that is available for pilfering.

2. Constraining Foreign Surveillance

Governments need to limit their own foreign spying to protect trust in an open, global internet. Governments can take steps, either unilaterally or multilaterally, to reduce concerns of foreign countries. If, for example, the focal point of the U.S. concern with Chinese companies is Chinese statutes that empower the government to demand that companies within their jurisdiction comply with their requests for information, then perhaps China could alleviate those concerns by placing further constraints on such laws. In response to the allegations against TikTok's foreign operations, Chinese Foreign Ministry Spokesperson Guo Jiakun stated on January 17, 2025 that "We have never and will never require any company or individual to collect or provide data, information, or intelligence located in foreign countries for the Chinese government in violation of local laws."[427] China could clarify its laws accordingly. The United States can lead the way, modeling limitations on foreign mass surveillance (including reform of the Foreign Intelligence Surveillance Act) and providing remedies for violations.[428]

---

424. *See* Faison, *supra* note 86, at 140 (arguing for a national comprehensive privacy law to address the problem of foreign surveillance "at its source—i.e. what data can be collected and what companies can do with that data").

425. DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAWS FAIL AND HOW TO IMPROVE IT 142 (2022).

426. *Id*. at 146 (emphasis omitted).

427. 2025 Nián 1 yuè 17 rì àijiāo bù fāyán rén guōjiākūn zhǔchí lì xíng jìzhě huì (2025年1月17日外交部发言人郭嘉昆主持例行记者会) [*Foreign Ministry Spokesperson Guo Jiakun's Regular Press Conference on January 17, 2025*], EMBASSY OF THE PEOPLE'S REPUBLIC OF CHINA IN THE KINGDOM OF NORWAY (Jan. 17, 2025), https://no.china-embassy.gov.cn/lcbt/wjbfyr/202501/t20250117_11537997.htm [https://perma.cc/XY9H-E5SG].

428. *See* Daskal, *supra* note 301, at 343–54 (discussing how, when FISA was initially passed in 1978, "the warrant requirement applied to citizens and noncitizens alike"); Daniel Severson, Note, *American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic*

There is precedent for governments revising their own surveillance rules to reduce the concerns of foreigners. In response to the global outcry regarding U.S. surveillance following the Edward Snowden disclosures of NSA spying across the world, President Barack Obama issued Presidential Policy Directive 28 ("PPD-28") on "Signals Intelligence Activities" on January 17, 2014.[429] PPD-28 limited both the collection and use of electronic communications.[430] Congress then passed two statutes, the USA FREEDOM Act, which ended bulk collection of electronic communications under Section 215 of the PATRIOT Act,[431] and the Judicial Redress Act, signed into law in 2016, allowing EU/EEA nationals to sue the U.S. government under U.S. privacy law.[432]

The Snowden revelations hastened the demise of the adequacy decision facilitating data flow to the United States, and the above measures helped to win the United States another adequacy decision through the EU–US Privacy Shield.[433]

A possible model for constraining foreign surveillance might be found in the EU–US Data Privacy Framework.[434] It limits so-called "signals intelligence" by U.S. authorities, requiring intelligence activities to consider "privacy and civil liberties" and be conducted only when "necessary to advance a validated intelligence priority" and "only to the extent and in a manner that is proportionate" to that priority.[435] The Framework charges the Civil Liberties Protection Officer (CLPO) in the Office of the Director of National Intelligence to hear challenges to U.S. surveillance to determine whether U.S. laws were violated and, if so, the "appropriate remediation."[436] A new tribunal, the Data Protection Review Court, created under Article II of the Constitution, will then review decisions by the CLPO, with help from a "special advocate" with the requisite security clearance, who will "advocat[e] regarding the complainant's interest in the matter."[437] Unlike the Safe Harbor and the Privacy Shield which name the European Union

Change, 56 HARV. INT'L L.J. 465, 504–09 (2015) (suggesting reforms to U.S. surveillance law with respect to non-U.S. persons).

429. *See Presidential Policy Directive – Signals Intelligence Activities*, THE WHITE HOUSE: OFF. OF THE PRESS SECRETARY (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/TH9T-8AM5].

430. *See id.*

431. *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, § 201, 129 Stat. 268, 277 (2015).

432. *See* Judicial Redress Act of 2015, Pub. L. No. 114-126, § 2, 130 Stat. 282, 3493–3494 (2016).

433. *See Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision*, at 35, COM (2016) 16/EN WP 238 (Apr. 13, 2016) (describing the USA FREEDOM Act as part of the "accessible legal framework" under which U.S. signals intelligence is conducted); *id.* at 55 (welcoming the Judicial Redress Act's extension of redress rights to certain non-U.S. persons, while noting limitations).

434. *See* EU-US Data Privacy Framework, 2023 O.J. (L 231) 118; Exec. Order No. 14086, 87 Fed. Reg. 62283, 62283–84 (Oct. 14, 2022); DATA PRIVACY FRAMEWORK PROGRAM, https://www.dataprivacyframework.gov [https://perma.cc/N2LZ-A98R] (last visited Dec. 31, 2025).

435. EU-US Data Privacy Framework, 2023 O.J. (L 231) 118, ¶¶ 129–31; *see* Exec. Order No. 14086, 87 Fed Reg. at 62283.

436. EU-US Data Privacy Framework, 2023 O.J. (L 231) 118, ¶ 181; *see* Exec. Order No. 14086, 87 Fed. Reg. at 62290.

437. Exec. Order No. 14086, 87 Fed Reg. at 62290; EU-US Data Privacy Framework, 2023 O.J. (L 231) 118, ¶ 183.

as the sole beneficiaries of those arrangements,[438] the U.S. orders implementing the Data Privacy Framework are written to be expandable beyond the European Union. Executive Order 14086 implements the Data Privacy Framework by limiting surveillance with necessity and proportionality requirements and by banning surveillance to suppress criticism or dissent, silence individuals, or seek an advantage for U.S. corporations.[439]

One key focus of legislative reforms should be Section 702 of the Foreign Intelligence Surveillance Act (FISA), which permits the Attorney General and the Director of National Intelligence to target non-U.S. persons for foreign surveillance.[440] Section 702's procedures are designed largely to protect the information of U.S. persons that might be incidentally collected in this process.[441] Indeed, even many reform proposals seek to better protect U.S. persons from being caught up in such surveillance,[442] neglecting similar concerns of foreign persons. Section 702 has a sunset provision and expires if not reauthorized by April 2026.[443] Before it is reauthorized, it might be possible to enshrine the constraints on foreign intelligence found in Executive Order 14086 and the Data Privacy Framework into the law. Such a reform would seek a balance between national security needs and the protection of individual privacy rights, both for Americans and foreign nationals whose data might be collected under FISA Section 702.

---

438. *See, e.g.*, *Issuance of Safe Harbor Principles and Transmission to European Commission*, 65 Fed. Reg. 45666, 45666 (July 24, 2000) ("Both the Safe Harbor Principles and the FAQs ('the Principles') are intended to serve as authoritative guidance to U.S. companies and other organizations receiving personal data from the European Union."). The EU-U.S. Privacy Framework was designed by the U.S. Department of Commerce and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. *Data Privacy Framework (DPF) Overview*, DATA PRIVACY FRAMEWORK PROGRAM, https://www.dataprivacyframework.gov/Program-Overview [https://perma.cc/43W2-M6H8] (last visited Dec. 31, 2025).

439. Exec. Order No. 14086, 87 Fed. Reg. at 62283.

440. 50 U.S.C. § 1881a(a); *see Warrantless Surveillance Under Section 702 of FISA*, ACLU, https://www.aclu.org/issues/national-security/warrantless-surveillance-under-section-702-fisa [https://perma.cc/Z2XK-5YYW] (last visited Dec. 31, 2025). Similar reforms would be needed for Executive Order 12333. *Cf.* Mark M. Jaycox, *No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333*, 12 HARV. NAT'L SEC. J. 58, 102 (2021) (proposing reforms for Executive Order 12333 focused largely on protecting U.S. persons).

441. *See* 50 U.S.C. § 1881a(d).

442. *See, e.g.*, Emily Berman, *Reimagining Surveillance Law*, 2023 U. ILL. L. REV. 1235, 1286 (2023) (arguing for "replacing the 'reasonably believed to be outside the United States' standard with 'clear and convincing evidence that the target is outside the United States,' or some similar, relatively demanding, standard"); Brittany Adams, *Striking a Balance: Privacy and National Security in Section 702 U.S. Person Queries*, 94 WASH. L. REV. 401, 440 (2019) (arguing that "querying the databases with U.S. person identifiers to obtain U.S. person information is subject to a more stringent analysis [under the Fourth Amendment] than the government and the courts have previously found").

443. George W. Croner, *After a Bruising Battle, FISA Section 702 Lives On . . . Now Let the 2026 Section 702 Reauthorization Debate Begin*, UNIV. PA. CAREY L. SCH.: CTR. FOR ETHICS & THE RULE OF L. (June 6, 2024), https://www.penncerl.org/the-rule-of-law-post/after-a-bruising-battle-fisa-section-702-lives-on-now-let-the-2026-section-702-reauthorization-debate-begin [https://perma.cc/KZ3C-673D].

Japan, too, has provided additional protections against surveillance and law enforcement access to European data as part of its process of winning an adequacy ruling from the European Commission.[444] As the European Commission reported, Japan provided "assurances to the Commission regarding safeguards concerning the access of Japanese public authorities for criminal law enforcement and national security purposes, ensuring that any such use of personal data would be limited to what is necessary and proportionate and subject to independent oversight and effective redress mechanisms."[445] The Japanese government also instituted a new "complaint-handling mechanism to investigate and resolve complaints from Europeans regarding access to their data by Japanese public authorities," which is "administered and supervised by the Japanese independent data protection authority."[446] Japan also amended its basic data protection law, the Act on the Protection of Personal Information, and provided additional safeguards through Supplementary Rules to guarantee that data transferred from the European Union received special protections.[447]

B. MULTILATERAL RESPONSE: NO MASS-SPYING TREATY

States "enjoy a peacetime right to spy under international law."[448] But that right can be abused.[449] This Section argues that states should entrench further limits on covert spying by treaty.

Many will find the prospect of an international treaty to limit spying among the world's biggest powers fanciful. This is clearly the most ambitious solution to the problem of foreign surveillance, but it is worth pursuing. Such an agreement would require each state to modify its laws and regulations to limit the collection of personal data of ordinary citizens of foreign countries and to provide redress mechanisms whereby individuals could challenge violations of these restrictions.[450]

An important precedent can be found in the recent Declaration on Government Access to Personal Data Held by Private Sector Entities agreed to in 2022 by the

444. *See* European Commission, Press Release IP/19/421, European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows (Jan. 23, 2019) (noting steps Japan took prior to EU adequacy decision). The EU has also negotiated special protections for European persons' data in Israel, but these focus on standard privacy protections and not limits on government surveillance. *See* Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023, KT 10637 (Isr.).

445. European Commission, Press Release IP/19/421, European Commission Adopts Adequacy Decision on Japan, Creating the World's Largest Area of Safe Data Flows (Jan. 23, 2019) (emphasis omitted).

446. *Id.* (emphasis omitted).

447. Flora Y. Wang, *Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement*, 33 HARV. J.L. & TECH. 661, 672, 674 (2020).

448. Asaf Lubin, *The Liberty to Spy*, 61 HARV. INT'L L.J. 185, 189 (2020).

449. *See id.* at 191 (identifying four "categories of abusive spying: (1) spying as a means to advance personal interests; (2) spying as a means to commit an internationally wrongful act; (3) spying as a means to advance corporate interests; and (4) spying as a means to exploit post-colonial relations").

450. *See* Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328, 348–49 (2018); Case C-311/18, Data Prot. Comm'r v. Facebook Ir., ECLI:EU:C:2020:559, ¶¶ 45, 65, 191 (July 16, 2020).

Ministers at the Organization for Economic Co-operation and Development (OECD) meeting on the digital economy.[451] While the OECD does not include China, this agreement among the thirty-eight member states suggests at least that the U.S, European governments, and some other governments are willing to commit to restraints on their national security and law enforcement information gathering operations.[452] It explicitly commits to restraints "including situations where countries have the authority under their national legal framework to mandate that private sector entities provide data to the government when the private sector entity or data are not located within their territory."[453] It is thus precisely focused on the problem described here: governments that might compel companies within their power to turn over data on foreign citizens. Both the Budapest Convention on Cybercrime and the new UN Convention on Cybercrime require that government orders to compel information from parties in their jurisdiction satisfy requirements of proportionality.[454]

Another precedent can be found in a 2015 executive agreement between Presidents Barack Obama and Xi Jinping for their respective countries to avoid cyber-espionage against each other.[455] Reports suggest that the agreement, while imperfect, led to a "dramatic[]" reduction in cyber-attacks originating in China against U.S. entities.[456]

Skeptics will, of course, argue that such an agreement will only invite cheating. The risk of cheating is indeed serious. Any such agreement would require extensive monitoring. If one government attributed a massive surveillance operation to another, it should be able to present its evidence and demand that the second government prove that it was not responsible and, if needed, take steps against any perpetrators operating within its shores.

---

451. *Landmark Agreement Adopted on Safeguarding Privacy in Law Enforcement and National Security Data Access*, OECD (Dec. 14, 2022), https://www.oecd.org/en/about/news/press-releases/2022/12/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.html [https://perma.cc/9NV6-ER5M].

452. See *Members and Partners*, OECD, https://www.oecd.org/en/about/members-partners.html [https://perma.cc/Y7LS-JNW6] (last visited Dec. 31, 2025).

453. OECD, DECLARATION ON GOVERNMENT ACCESS TO PERSONAL DATA HELD BY PRIVATE SECTOR ENTITIES 6 (Dec. 13, 2022).

454. Council of Eur., Budapest Convention on Cybercrime, Nov. 23, 2021, E.T.S. No. 185, art. 15 (requiring safeguards of proportionality for government authorities exercising powers and procedures for obtaining information); G.A. Res. 79/243, U.N. Doc. A/AC.291/L.15, Draft United Nations Convention Against Cybercrime, art. 24 (Aug. 7, 2024) (same).

455. *See* David E. Sanger, *Chinese Curb Cyberattacks on U.S. Interests, Report Finds*, N.Y. TIMES (June 20, 2016), https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html.

456. *Id.* ("Nine months after President Obama and President Xi Jinping of China agreed to a broad crackdown on cyberespionage aimed at curbing the theft of intellectual property, the first detailed study of Chinese hacking has found a sharp drop-off in almost daily raids on Silicon Valley firms, military contractors and other commercial targets."). The report noted, "We still see semiconductor companies and aerospace firms attacked." *Id.* (internal quotation marks omitted). In 2018, a National Security Agency official accused China of violating the 2015 agreement while also noting that "the quantity and number of attacks had dropped 'dramatically' since the agreement." *U.S. Accuses China of Violating Bilateral Anti-Hacking Deal*, REUTERS (Nov. 9, 2018, at 03:06 EST), https://www.reuters.com/article/world/us-accuses-china-of-violating-bilateral-anti-hacking-deal-idUSKCN1NE041.

There is reason to think that geopolitical rivals might find common ground on restraining each other's signals intelligence. As one security expert noted regarding the earlier Obama-Xi agreement, "while there are serious differences, there are also common interests."[457] After all, China, too, must worry about foreign governments snooping on its citizens. In 2012, Edward Snowden provided documents to a Hong Kong newspaper that reportedly showed that U.S. intelligence services had hacked into the networks of Tsinghua, China's most prestigious university and home to one of six backbone networks in the nation.[458] Snowden also claimed that the NSA had hacked Chinese telecommunications networks, gaining access to millions of text messages.[459]

Microsoft's Brad Smith has proposed a Digital Geneva Convention to "commit governments to implement the norms that have been developed to protect civilians on the internet in times of peace."[460] Smith would require that governments "report [cybersecurity] vulnerabilities to vendors rather than stockpile, sell or exploit them."[461] Smith also suggests the creation of an international organization that can investigate and publicly attribute nation-state attacks.[462] The proposal of an anti-digital spying treaty offered here would expand on Smith's suggestion by including prohibitions not just on cyberattacks, but also on legal orders to compel the disclosure of personal information of foreign persons without sufficient checks and balances.

To summarize this Part: first, governments can take confidence building steps by limiting their own mass spying on foreign peoples, hoping to gain trust for their own enterprises; second, governments can work together to limit spying.

CONCLUSION

Checkpoint Charlie was enforced by the gun. Troops along the Eastern side of the Berlin Wall had orders to shoot if "there was no other way to make an

457. James Andrew Lewis, *Moving Forward with the Obama-Xi Cybersecurity Agreement*, CTR. FOR STRATEGIC & INT'L STUD. (Oct. 21, 2015), https://www.csis.org/analysis/moving-forward-obama-xi-cybersecurity-agreement [https://perma.cc/FA5U-7PGR].

458. *See* Lana Lam, *Exclusive: NSA Targeted China's Tsinghua University in Extensive Hacking Attacks, Says Snowden*, S. CHINA MORNING POST (Aug. 13, 2013, at 15:45 ET), https://www.scmp.com/news/china/article/1266892/exclusive-nsa-targeted-chinas-tsinghua-university-extensive-hacking [https://perma.cc/UKT3-NNB6]; Andrew Jacobs, *After Reports on N.S.A., China Urges End to Spying*, N.Y. TIMES (Mar. 24, 2014), https://www.nytimes.com/2014/03/25/world/asia/after-reports-on-nsa-china-urges-halt-to-cyberspying.html.

459. Lana Lam & Stephen Chen, *Exclusive: US Spies on Chinese Mobile Phone Companies, Steals SMS Data: Edward Snowden*, S. CHINA MORNING POST (June 23, 2013, at 19:20 ET), https://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden [https://perma.cc/5E45-78WN].

460. *A Cloud for Global Good*, MICROSOFT (2018), https://news.microsoft.com/cloudforgood/policy/microsofts-commitment.html [https://perma.cc/4D7C-FJV8] (providing policy recommendations to governments and other industries in using cloud-powered technology); *see* Smith, *supra* note 191.

461. *A Cloud for Global Good*, *supra* note 460.

462. *Id.*

arrest."[463] Today's Digital Walls are not enforced by violence. Instead of visible walls, we have obscure legal texts and administrative rulings that enforce Digital Walls. But these digital borders have enormous consequences for humanity nonetheless.

The internet did not come with national borders built in. These are being retrofitted in. In 2022, *The New York Times* published a story with a striking title: "The Era of Borderless Data Is Ending."[464] "France, Austria, South Africa and more than 50 other countries are accelerating efforts to control the digital information produced by their citizens, government agencies and corporations," the *Times* reported.[465] But the headline downplayed what was at stake: it is more than "borderless data" that is at risk—it is the global internet itself, and the twenty-first century trade and communication that it enables. As a major study of the Council of Foreign Relations concluded, "the era of the global internet is over."[466] The co-chair of this study was appointed as the nation's first "Cyber Ambassador," overseeing the newly-created Bureau of Cyberspace and Digital Policy at the U.S. State Department.[467]

Alarm over real foreign threats is, understandably, driving this reconfiguration. Built to enable communications even in the face of catastrophe, the internet is being refashioned to serve national security. But these new digital firewalls may prove both ineffective and dangerous. In February 2024, reports indicated that nearly half of the population of France had their medical insurance records hacked.[468] The hackers were able to access the records held by two French service providers for medical insurance companies.[469] Neither the fact that the companies were French nor the fact that the data was retained on French soil guaranteed the safety of the data. In August 2024, Russian hackers were among those released by the United States in a prisoner exchange for journalist Evan Gershkovich and other Americans.[470] They hacked U.S. companies from abroad to access

---

463. *Victims of the Wall*, BERLIN, https://www.berlin.de/mauer/en/history/victims-of-the-wall [https://perma.cc/33AW-L37K] (last visited Dec. 31, 2025). For short biographies of the 140 people killed at the border, see *Todesopfer* [*Fatalities*], CHRONIK DER MAUER, https://www.chronik-der-mauer.de/todesopfer [https://perma.cc/BCN5-892D] (last visited Dec. 31, 2025).

464. David McCabe & Adam Satariano, *The Era of Borderless Data Is Ending*, N.Y. TIMES (May 23, 2022), https://www.nytimes.com/2022/05/23/technology/data-privacy-laws.html.

465. *Id.*

466. NATHANIEL FICK, JAMI MISCIK, ADAM SEGAL & GORDON M. GOLDSTEIN, COUNCIL ON FOREIGN RELS., CONFRONTING REALITY IN CYBERSPACE: FOREIGN POLICY FOR A FRAGMENTED INTERNET at vii (2022).

467. *See* Tim Starks, *Cyber Ambassador Could Soon Take on a World of Challenges*, WASH. POST (Aug. 2, 2022), https://www.washingtonpost.com/politics/2022/08/02/cyber-ambassador-could-soon-take-world-challenges.

468. Oceane Duboust, *Data of Half the Population of France Stolen in Its Largest Ever Cyberattack. This Is What We Know*, EURONEWS (Feb. 8, 2024, at 20:44 GMT), https://www.euronews.com/next/2024/02/08/data-of-33-million-people-in-france-stolen-in-its-largest-ever-cyberattack-this-is-what-we [https://perma.cc/6F28-Y7JV].

469. *Id.*

470. *See* Kevin Collier, *Release of Russian Hackers Believed to Be First U.S. Prisoner Swap to Include International Cybercriminals*, NBC NEWS (Aug. 1, 2024, at 17:34 EDT), https://www.nbcnews.com/tech/security/us-releases-russian-hackers-evan-gershkovich-prisoner-swap-rcna164746 [https://

confidential earnings reports and exploit that inside information in the stock market.[471] They were arrested while on vacation in Switzerland and the Maldives.[472] After the hacking of U.S. telecom networks of companies like AT&T and Verizon in 2024 in the "Salt Typhoon" hack often ascribed to Chinese actors, the U.S. government redoubled its rip and replace efforts in telecommunications, targeting Chinese equipment.[473] But the security vulnerabilities seem not to have emanated from Chinese equipment, but from equipment by U.S. networking giant Cisco and U.S. security company Fortinet.[474] Critiquing European proposals to reject American companies from receiving European cybersecurity certification, the U.S. group the Business Software Alliance spokesman observed: "Good cybersecurity doesn't come from where a company is headquartered, it comes from how well its systems are built and maintained."[475] This is true for U.S.-based companies supplying Europe, but also for Chinese companies supplying the United States.

A decade ago, the U.S. military conceptualized "cyber" as the fifth domain of war, alongside land, sea, air, and space.[476] Over the last few decades, the word "cyber" has transformed from denoting a space for endless possibility, to a domain of foreign threat actors. As we respond to the threat actors operating relentlessly across global digital networks, we should be careful not to sacrifice our freedoms in the process.

---

perma.cc/XP7B-8S7X]. On August 1, 2024, the U.S. released two Russian hackers in exchange for Evan Gershkovich and other Americans. *See id.*

471. *Id.*

472. *Id.*

473. *See* David E. Sanger, Julian E. Barnes, Devlin Barrett & Adam Goldman, *Emerging Details of Chinese Hack Leave U.S. Officials Increasingly Concerned*, N.Y. TIMES (Nov. 22, 2024), https://www.nytimes.com/2024/11/22/us/politics/chinese-hack-telecom-white-house.html.

474. *See* Dustin Volz, Aruna Viswanatha, Sarah Krouse & Drew FitzGerald, *How Chinese Hackers Graduated from Clumsy Corporate Thieves to Military Weapons*, WALL ST. J. (Jan. 4, 2025, at 21:00 ET), https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95 ("In the telecom attacks, the hackers exploited unpatched network devices from security vendor Fortinet and compromised large network routers from Cisco Systems."); Lucie Cardiet, *The Silent Storm: Inside Salt Typhoon's Massive Telco Cyberattack*, VECTRA AI: HYBRID ATTACK BULL. (Dec. 12, 2024), https://www.vectra.ai/blog/the-silent-storm-inside-salt-typhoons-massive-telco-cyberattack [https://perma.cc/4MLF-UB4F] ("Salt Typhoon has been observed exploiting Cisco-specific features and defaults."). One telecom security expert argued that rip and replace would not be a cost effective approach to respond to Salt Typhoon: "Most of these intrusions took advantage of decades-old security architecture flaws and exploited known cyber hygiene issues like missing patches or vulnerable accounts and leaked passwords." David DiMolfetta, *GAO Mulls Cost Evaluation of Nationwide Telecom Hardware Replacement*, NEXTGOV/FCW (Jan. 6, 2025), https://www.nextgov.com/cybersecurity/2025/01/gao-mulls-cost-evaluation-nationwide-telecom-hardware-replacement/401963 [https://perma.cc/SE8V-HE2A] (statement of Marc Rogers, a thirty-five year telecom security practitioner).

475. *EU: Cybersecurity Policy Must be About Protection, Not Protectionism*, BUS. SOFTWARE ALL. (June 19, 2025), https://www.bsa.org/news-events/news/eu-cybersecurity-policy-must-be-about-protection-not-protectionism [https://perma.cc/8WXP-FZU8].

476. DEP'T DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 5 (2011).