Draft, January 19, 2025

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 have innovated a new tool of international border control—what I call "data localization squared." Now, not only must data be stored on local servers, it must be stored on local servers owned and operated by local companies. This is operationalized through a new legal tool, not previously discussed in legal scholarship: a requirement for immunity from foreign jurisdiction. We are witnessing the creation of Digital Berlin Walls, complete with Checkpoint Charlies to permit border crossings.

The Article traces this turn through five case studies: TikTok, the Chinese "Delete America" program, the U.S. "rip and replace" program, Microsoft's Office 365, and connected cars. The national security turn now affects digital services and modern goods, and with it issues such as economic development and climate change.

This Article identifies the rise of a new tool of transnational control—immunity from foreign jurisdiction—which has not been previously discussed in legal scholarship. Governments keen to avoid their citizens' data from falling into the hands of foreign governments now demand not only that personal data be stored on local servers, it must be stored on local servers by local companies—what this Article describes as "data localization squared." The ascent of digital border controls in the name of national security treats a domain of speech and commerce with the rules of war.

The Article argues that the national security internet will come at a price, disrupting trade and investment, reducing competition, inviting retaliation, increasing government control over speech, and impeding in global collaboration to stem climate change, while offering easily circumvented protection against foreign surveillance. The Article offers a typology of efforts by corporations to satisfy national security demands and identifies the weaknesses of each approach. The Article proposes reforms that constrain foreign surveillance in order to protect both civil rights and national security.

---

* Scott K. Ginsburg Professor of Law and Technology, Georgetown University. I thank Anu Bradford, William Dodge, and Paul Schwartz for invaluable insights, Donara Aghajani, Daniel Csigirinszkij, Kurtis Lee, Chao Li, Bo Peng, Virginia Polik, and Daniel Powell at Georgetown and Irene Kim at Harvard for excellent research assistance, and commentators at a workshop at the Institute for Rebooting Social Media at Harvard for very helpful comments. 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 188 and accompanying text.

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. Before transferring data out of China, many companies now need to pass an explicit "Data Exit Security Assessment."[1]

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. The United States has brought a growing arsenal of international economic law tools—from international emergency economic powers, to foreign investment reviews, to export controls—to scrutinize the outward flow of data on national security grounds.[2] 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.[3] The Biden Administration's Executive Order on Artificial Intelligence includes an array of measures designed to prevent foreign adversary nations from accessing advanced AI services.[4] The U.S. has employed foreign investment reviews to unwind a Chinese acquisition of the dating app Grindr and to reject a Chinese acquisition of MoneyGram.[5] Most famously, in April 2024, the U.S. 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.[6]

---

[1] *China: CAC issues Data Export Security Assessment Measures*, ONETRUST DATA GUIDANCE, https://www.dataguidance.com/news/china-cac-issues-data-export-security-assessment (last visited Feb. 12, 2023); Outbound Data Transfer Security Assessment Measures, *translated in* DIGICHINA (Oct. 29, 2021), https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/.

[2] *See* Exec. Order No. 14,117, 89 Fed. Reg. 15421 (Feb. 28, 2024) (calling for regulations to prevent the transfer of sensitive personal data and the United States government-related data to countries of concern).

[3] American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. § 4(b)(8) (requiring disclosure if covered data is made available in an adversary country such as China). An earlier bipartisan privacy bill also included a nearly identical provision. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. §202(b)(9) (2022).

[4] Exec. Order No. 14,110, 88 Fed. Reg. 75191, 75198 (Nov. 1, 2023) (Directing the Secretary of Commerce to propose regulations requiring advanced AI providers to submit a report when conducting foreign transactions, restrict foreign resellers, verify the identity of any foreign lessee)

[5] Yuan Yang in Beijing & James Fontanella-Khan, *Grindr sold by Chinese owner after US national security concerns*, FIN. TIMES, Mar. 7, 2020, https://www.ft.com/content/a32a740a-5fb3-11ea-8033-fa40a0d65a98. 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 (Trump Administration's expansion of CFIUS blocks Ant Financial's purchase of MoneyGram)

[6] Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, § H (2024).

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.[7] But as the TikTok example demonstrates, localizing data on domestic servers (as TikTok offered through its Project Texas mitigation proposal)[8] 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 emergence of a new legal doctrine—*immunity from foreign jurisdiction*—which requires 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—to rules on ownership in broadcasting, telecommunications, and critical infrastructure. France's national cybersecurity agency, for example, explicitly 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.[9] 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."[10] Google and Microsoft can provide cloud services, but only as long as they license their technologies to French companies, he continued. The key requirement: the data cannot become accessible to companies subject to U.S. jurisdiction. Quite simply: Foreign service providers need not apply.

These extraordinary demands reflect growing anxieties about geopolitical conflicts and real concerns about excessive foreign surveillance.[11] These efforts began in earnest after the Snowden revelations of 2013, which showed the extent of U.S. foreign surveillance operations, but have increased with revelations suggesting Russian election-related hacking of U.S. politicians and possible Chinese hacking of the U.S. Office of Personnel Management.[12] 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. Rather than the foundation for global speech and economic

---

[7] *See, e.g.,* Anupam Chander & Uyên P. Lê, *Data Nationalism,* 64 EMORY L.J. 677, 680 (2015).

[8] ByteDance Ltd., TikTok Ltd., TikTok Inc., TikTok U.S. Data Security Inc. & CFIUS Monitoring Agencies, Draft National Security Agreement §§11.5, 11.8-.10 (Parties' Draft as of 8/23/22) (hereinafter "Draft National Security Agreement").

[9] Agence Nationale de la Sécurité des Systèmes d'Information, *Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences*, Version 3.2.a, Sept. 21, 2021, art. 19.6.; unofficial translation at https://www2.itif.org/2021-secnumcloud-3.2.a-english-version.pdf. *See also* Dominique Luzeaux, *Cloud souverain: souveraineté et résilience, ou confiance?*, 855 REVUE DÉFENSE NATIONALE 14 (2022) (paper by director of the French Defense Digital Agency, arguing for national self-reliance rather than dependence on trusted, often foreign, partners).

[10] Mathieu Rosemain, *France embraces Google, Microsoft in quest to safeguard sensitive data*, REUTERS, May 17, 20218:24 AM ED, https://www.reuters.com/technology/france-embraces-google-microsoft-quest-safeguard-sensitive-data-2021-05-17/.

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

[12] *See e.g.,* Julian E. Barnes & Edward Wong, *In Risky Hunt for Secrets, U.S. and China Expand Global Spy Operation,* N.Y. TIMES, Sept 17, 2023, https://www.nytimes.com/2023/09/17/us/politics/us-china-global-spy-operations.html.

prosperity,[13] cross-border data flows are now seen as a national security threat. This concern echoes through the halls of power from Beijing to Berlin, and from New Delhi to Washington, D.C. The idea of an open and free global internet has gradually been replaced by a splinternet, and the "Pax Americana" of a global internet of free flows[14] replaced by a growing reality of national security border controls, embraced by the United States itself.

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. Designing a communications network to be "survivable … even in the thermonuclear war" meant avoiding any "central--and therefore vulnerable--control point."[15] 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 that 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 while minimizing the harms of a national security internet. The "National Security Internet" described here reflects the extension of the aggrandizement of the executive branch over foreign affairs that Harold Koh seeks to control through what he calls the "National Security Constitution," where the legislative and judicial branches play a disciplinary role in foreign affairs.[16] 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. International trade, especially the digital trade that is an increasingly vital part of the world economy, is at risk as data must now undergo a border security check. Data insecurity threatens to tear the internet apart into separate trading zones.[17] In a new book, Anu Bradford argues that the U.S., EU, and China are promulgating three digital empires, based on incompatible visions of the internet.[18] This Article argues that even while the three may be seeking to export their visions, they are simultaneously building digital firewalls between their own empires, threatening both trade and information flows. 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

---

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

[14] Paul Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1684 (2018).

[15] Paul Baran, *On Distributed Communications: I. Introduction to Distributed Communications Networks* V, 16 (Rand Corp., Aug. 1964).

[16] HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION IN THE TWENTY-FIRST CENTURY (2024).

[17] 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 (2018); Henry Gao, *Data Sovereignty and Trade Agreements: Three Digital Kingdoms* in ANUPAM CHANDER & HAOCHEN SUN, DATA SOVEREIGNTY: FROM THE DIGITAL SILK ROAD TO THE RETURN OF THE STATE 213 (2023).

[18] ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY (2023).

enterprise operating in the United States could not be owned by a company from China for fear that the data might flow with ownership.[19] But even as the U.S. kicks out the Chinese owners of TikTok, China is seeking to "delete America" from the government's technology stack.[20]

Not just software, but also to modern goods trade, which is increasingly reliant on cross-border data flows, stands at risk. The Biden Administration, for example, has raised national security concerns with the sale of Chinese cars within our borders, and some Members of Congress in a bipartisan letter to the Securities and Exchange Commission have questioned the operations of fast fashion company Shein, household goods company Temu, and drone manufacturer DJI because of their Chinese connections.[21]

International investments have been blocked because of the risk that data about a nation's citizens might fall into the wrong foreign hands.[22] After a U.S. divestiture order for a Chinese company's acquisition of a cloud-based hotel management software company, other

[19] Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (2020) (IEEPA executive order banning transactions with TikTok); *Presidential Order Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51297 (Aug. 14, 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. 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 272-280 and accompanying text.

[20] Liza Lin, *China Intensifies Push to 'Delete America' From Its Technology*, WALL ST. J. (Mar. 7, 2024), 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.").

[21] Letter from Rep. Jennifer Wexton *et al.* to Gary Gensler, Chair, Securities and Exchange Commission (May 1, 2023) (https://wexton.house.gov/uploadedfiles/2023-05-01_sec_letter.pdf). For its part, China requires data localization for Tesla's operations in China. China had already banned Tesla cars from certain government buildings for fear that they may transmit secrets to foreign powers. Cheng Ting-Fang & Shunsuke Tabeta, *Tesla cars face more entry bans in China as 'security concerns' accelerate*, NIKKEI, Jan. 24, 2024, 11:35 JST, https://asia.nikkei.com/Spotlight/Supply-Chain/Tesla-cars-face-more-entry-bans-in-China-as-security-concerns-accelerate; Heather Somerville, *Why First Responders Don't Want the U.S. to Ban Chinese Drones*, WALL ST. J., Aug. 7, 2024 8:30 am ET, https://www.wsj.com/politics/national-security/congresss-plan-to-outlaw-chinese-drones-met-with-protest-c95cf1fe?mod=hp_listc_pos2

[22] In 2019 the Committee on Foreign Investment in the United States ordered the divestiture of the dating app Grindr, as well as online health service PatientsLikeMe, both of which had been acquired by Chinese entities. 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), https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html. Earlier, in 2017, Ant Financial, the financial arm of China-based Alibaba, had its acquisition of MoneyGram blocked over data concerns. Greg Roumeliotis, *U.S. blocks MoneyGram sale to China's Anti Financial on national security concerns,* REUTERS (Jan. 3, 2018), https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial-idUSKBN1ER1R7.

companies worried about all Chinese acquisitions because "almost every American company collects data on its users."[23]

The issue even threatens international financial markets. Chinese companies offering registered securities in the U.S. 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.[24] 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. securities disclosure requirements.[25] 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 U.S. 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."[26] Accordingly, some of the largest Chinese companies announced plans to delist from the New York exchanges.[27] Didi's initial public offering in New York led to a Chinese government backlash that led Didi to delist from the NY Stock Exchange "due to [Chinese government] worries about leakage of sensitive data."[28] The standoff between the governments was alleviated when China permitted U.S. regulators to access audit data,[29] but the pause may only be temporary.[30] Fashion giant Shein's planned 2024 IPO in New York was foiled by

---

[23] 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.

[24] Lulu Yilun Chen & John Cheng, *China State-Owned Giants to Delist From US Amid Audit Spat*, BLOOMBERG, Aug. 12, 2022, https://www.bloomberg.com/news/articles/2022-08-12/china-state-owned-giants-plan-to-delist-from-us-amid-audit-spat?leadSource=uverify%20wall.

[25] Holding Foreign Companies Accountable Act, Pub. L. No. 166-222, §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).

[26] Chen & Cheng, *supra* note 24.

[27] Five major Chinese companies, including 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.*

[28] Julie Zhu, Kane Wu and Brenda Goh, *Beijing presses Didi to delist from U.S. over data security fears* (Nov. 26, 2021, 9:39 AM CST), https://www.reuters.com/world/china/china-asks-didi-delist-us-security-fears-bloomberg-news-2021-11-26/; Shiyi Chen & Coco Liu, *Didi's Move From NYSE to Hong Kong – What to Know*, BLOOMBERG (Dec. 3, 2021, 12:18 AM EST), https://www.bloomberg.com/news/articles/2021-12-03/everything-we-know-about-didi-s-plan-to-delist-from-the-nyse.

[29] Laura He, *Delisting risks for China tech stocks averted as US gets 'historic' access to audit data,* CNN (Dec. 16, 2022, 1:09 AM EST), https://www.cnn.com/2022/12/16/business/china-stock-us-delisting-averted-audit-access-intl-hnk/index.html.

[30] Jesse M. Fried & Tamar Groswald Ozery, *The Holding Foreign Companies Accountable (HFCA) Act: A Critique* 16-17 (Eur. Corp. Governance Inst. – Law Working Paper no. 721, 2023),

cybersecurity concerns—both in the United States and China.[31] After facing backlash from U.S. lawmakers, Shein scrapped its efforts for a US IPO and has filed paperwork for an IPO on the London Stock Exchange.[32] However, Shein has attracted increasing scrutiny from U.K. law makers amid concerns of its origins in China, its China-based supply chain, and addition to fast-fashion waste. Should the London based IPO fail, Shein is considering a Hong Kong based IPO which has potentially dramatic consequences for the initial valuation Shein can secure.[33]

This Article builds on existing literatures. Mark Lemley worries about the harms of the "Splinternet."[34] Kristen Eichensehr and Cathy Hwang describe the security creep in U.S. foreign investment law.[35] Kathleen Claussen observes that U.S. national security law permits the erection of barriers that seemingly undermine trade, but argues that national security authorities have become unmoored from their original purposes.[36] J. Benton Heath highlights the security creep in international trade law.[37] Mona Pinchis-Paulsen sheds light on the interpretation of the national security exception in modern trade law through a study of its historical origins.[38] Neha Mishra argues that cybersecurity measures that governments are now taking that disadvantage foreign suppliers may not be able to successfully avail themselves of the national security exceptions in trade law.[39] Uyên P. Lê and I have cautioned against threats to both civil and economic liberties from emerging practices of data localization.[40] Paul Schwartz has observed the panoply of U.S. legal authorities that permit parties to seek data held abroad.[41] Paul Schwartz and I have observed the rising conflict between data privacy and trade,[42] and the national security turn in U.S. data policy.[43] Ganesh Sitaraman defends the national security turn in regulating foreign platforms based on what he finds is a long history

---

http://ssrn.com/abstract_id=4505890 (arguing that Chinese authorities might again refuse access to such records in the future).

[31] Liza Lin & Raffaele Huang, *Fashion Giant Faces New IPO Hitch: China's Cybersecurity Police,* WALL ST. J. (Jan. 16, 2024, 10:50 pm ET), https://www.wsj.com/world/china/fashion-giant-faces-new-ipo-hitch-chinas-cybersecurity-police-70c57561.

[32] *Id.*

[33] James Fontanella-Khan et. al, *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.

[34] Mark Lemley, *The Splinternet*, 70 DUKE L. J. 1397, 1399 (2021) ("The balkanization of the internet is a bad thing, and we should stop it if we can.").

[35] Kristen Eichensehr & Cathy Hwang, *National Security Creep in Corporate Transactions*, 123 COLUM. L. REV. 549 (2023).

[36] Kathleen Claussen, *Trade's Security Exceptionalism*, 72 STAN. L. REV. 1097, 1142 (2020).

[37] J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L.J. 1020 (2020).

[38] 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).

[39] Neha Mishra, *The Trade–(Cyber)security Dilemma and its Impact on Global Cybersecurity Governance*, 54 J. WORLD TRADE 567 (2020).

[40] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. J. 677 (2015).

[41] Schwartz, *supra* note 14.

[42] Anupam Chander & Paul Schwartz, *Privacy and/or Trade*, 90 U. CHI. L. REV. 49 (2023).

[43] Anupam Chander & Paul Schwartz, *The President's Authority over Cross-Border Data Flows*, PENN. L. REV. (forthcoming 2024) (draft available upon request).

of similar actions.[44] Henry Farrell and Abe Newman incisively show the weaponization of international economic tools by the United States.[45] 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 software is eating the world,[46] national security is now eating software.[47]

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, the European Union, and China. Part II reviews flashpoints demonstrating this national security turn in internet regulation, going from TikTok to Office 365 to cars and cranes.

Part III argues that broad national security firewalls are expensive, harm trade, intrusive, undermine competition, easy to evade, 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,[48] we should worry about the rise of national security controls over the internet. Such expanded national security

---

[44] Ganesh Sitaraman, *The Regulation of Foreign Platforms*, 74 STAN. L. REV. 1073 (2022).

[45] HENRY FARRELL AND ABRAHAM NEWMAN, UNDERGROUND EMPIRE: HOW AMERICA WEAPONIZED THE WORLD ECONOMY (2023).

[46] 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/.

[47] 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 (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).

[48] *See, e.g.,* DAVID COLE & JAMES DEMPSEY, TERRORISM AND THE CONSTITUTION: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY 195-218 (2006); *but see* Adrian Vermeule, *Self-Defeating Proposals: Ackerman on Emergency Powers*, 75 FORDHAM L. REV. 631, 632, 634 (2006) (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."); *see also* Lisa Finnegan Abdolian & Harold Takooshian, *The USA Patriot Act: Civil Liberties, the Media, and Public Opinion*, 30 FORDHAM URB. L.J. 4 (2003); Jacob R. Lilly, *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 CORNELL J.L. & PUB. POL'Y 2 (Spring 2003); Caspar Bowden, *The US surveillance programmes and their impact on EU citizens' fundamental rights,* Eur. Parl. PE 474.405 (2013); Privacy and Civil Liberties Oversight Board, *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*, Jan. 23, 2014; Office of the Inspector General, *A Review of the Federal Bureau of Investigations Use of National Security Letters* (Mar. 2007); Robert Graves & Indranil Ganguli, *Extraterritorial Application of the USA PATRIOT Act and Related Regimes: Issues for European Banks Operating in the United States*, PRIV. & SEC. L.J. (Oct. 2007); Christopher Raab, *Fighting Terrorism in an Electronic Age: Does the Patriot Act Unduly Compromise our Civil Liberties?*, 2 DUKE L. & TECH. Rev. (2006).; James M Lutz & Georgia Wralstad Ulmschneider, *Civil Liberties, National Security and U.S. Courts in Times of Terrorism*, 13 PERSP. ON TERRORISM 6 (Dec. 2019).

controls often offer what Shirin Sinnar has called "rule of law tropes," measures that hide excessive executive powers behind a regulatory façade.[49] Part IV builds on Kristen Eichensehr's concept of "Digital Switzerlands" to show how companies are attempting to navigate global geopolitics. Part V proposes restraints on foreign surveillance to address the core concerns animating the national security internet.

I. THE RISE OF DIGITAL BERLIN WALLS

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. The Great Firewall of China is now met by the Digital Berlin Walls of the United States and Europe. While the notion of a Chinese digital firewall will seem familiar, this Part shows that even it has expanded from a system focused on censorship to a system also focused on thwarting foreign surveillance.

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. The U.S. 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.[50] Some saw in the proposal an effort to create a "no-China club" internet.[51] Facing pushback from its international partners, the U.S. ultimately opted for a broader Declaration for the Future of the Internet that "reaffirms and recommits its partners to a single global Internet."[52]

This Part focuses on three jurisdictions--the United States, China, and the European Union—chosen because they represent the world's three largest economies. While our focus is on these three jurisdictions, the issue arises beyond the three jurisdictions in this study. For example, India banned Chinese apps for excessive data collection about Indians as an explicit "digital strike" in response to the literal hurling of stones between Chinese and Indian troops

[49] 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 (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).

[50] Shirin Sinnar, *Rule of Law Tropes in National Security*, 129 HARV. L. REV. 1566, 1568 (2016).

[51] *Id.* (quoting Graham Webster, editor-in-chief of the DigiChina Project at the Stanford University Cyber Policy Center).

[52] *Declaration for the Future of Cyberspace,* U.S. DEP'T OF STATE, https://www.state.gov/declaration-for-the-future-of-the-internet (last visited Feb. 13, 2024).

in the Himalayas.[53] The Japanese messaging company Line faced criticism when it was revealed that some in China had access to data of Line users.[54]

This Part begins by showing the growing arsenal of legal tools that the U.S. is assembling to stop data flows across the border in the interest of national security. It then shows the evolution of China's Great Firewall, from promoting censorship to protecting against foreign surveillance. A third section shows that the European Union, too, has implemented protections against foreign surveillance but it has done so through data protection law, not national security law. This Part concludes with a definition and analysis of the emerging doctrine of immunity from foreign jurisdiction.

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.[55] The *New York Times* went further, arguing the internet might balkanize into three zones—the U.S., Chinese, and European internets.[56] One author, writing for the Council on Foreign Relations, encouraged the U.S. to "weaponize digital trade," creating a digital trade zone that would exclude China through a "democratic digital supply chain," excluding Chinese software and hardware.[57] The author would become the architect of the Biden Administration's national cyber strategy at the Office of the National Cyber Director.[58]

The U.S. 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

---

[53] *'Banning Chinese apps a digital strike': Union Minister Ravi Shankar Prasad*, HINDUSTAN TIMES (July 2, 2020), https://www.hindustantimes.com/india-news/banning-chinese-apps-a-digital-strike-union-minister-ravi-shankar-prasad/story-XQQbTVt4bauqeBHfXC75iM.html.

[54] Kenji Minemura & Toshiya Obu, *Personal data of millions of Line users accessed by affiliate in China*, ASAHI SHIMBUN (Mar. 17, 2021, 19:38 JST), https://www.asahi.com/ajw/articles/14276271. Line had contracted with another Japanese company to review notifications of inappropriate posts, and that company had subcontracted with a Chinese company to review the posts, leading to the risk of inappropriate access. *Id.* 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 (May 7, 2022, 03:25 JST), https://asia.nikkei.com/Business/Technology/Japan-to-label-cloud-services-as-critical-for-economic-security. Brazil's Supreme Court has upheld the power to compel companies to turn over data held abroad. Shanzay Pervaiz & Alex Joel, *Data Localization and Government Access to Data Stored Abroad: Discussion Paper 2*, Joint PIJIP/TLS Rsch. Paper Series at 5 (2023), https://digitalcommons.wcl.american.edu/research/87.

[55] Lora Kolodny, *Former Google CEO Predicts the Internet Will Split in Two—and One Part Will Be Led by China*, CNBC (Sept. 20, 2018), http://cnbc.com /2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html ("most likely scenario now is … a bifurcation into a Chinese-led internet and a non-Chinese internet led by America").

[56] Editorial Board, *There May Soon Be Three Internets. America's Won't Necessarily Be the Best*, NY TIMES, Oct. 15, 2018, http://nytimes.com/2018/10/15/opinion/internet-google-china-balkanization.html.

[57] Robert K. Knake, *Weaponizing Digital Trade: Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity* (Council on Foreign Relations, Special Report No. 88, September 2020).

[58] Suzanne Smaley, *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.

is the International Emergency Economic Powers Act of 1977 (IEEPA), which provides the President and the executive branch broad powers to take steps to respond to international economic emergencies.[59]

The President's invocation of IEEPA to staunch cross-border data flows is complicated by a significant exception to this statute. In 1988, Congress amended IEEPA to explicitly exclude the cross-border transfer of "informational materials" from the authority granted to the President under the statute.[60] What would come to be known as the Berman Amendment, after its sponsor, Representative Howard Berman, excluded "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…."[61] 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."[62] Congress trusted the American people to make up their own mind, even after exposure to foreign propaganda.[63]

The informational materials exception did 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

[59] 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 SECURITY (May 24, 2019), https://www.justsecurity.org/64252/an-emergency-or-business-as-usual-huawei-and-trumps-emergency-powers/.

[60] 50 U.S.C. §§ 1702(b)(3). The original version of the statute, as passed in 1977, had 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. P.L. 95-223 (December 28, 1977). This remains in the statute today.

[61] PL 100–418 (HR 4848), § 2502(a)(1), Aug. 23, 1988, 102 Stat 1107, 1371.

[62] Note, Tracy J. Chin, *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 clear that the legislation sought to remove "barriers that inhibit the free exchange of ideas across international frontiers." 132 Cong. Rec. 6550, 6550 (1986) (cited in Note, Laura A. Michalec, *Trade with Cuba Under the Trading with the Enemy Act: A Free Flow of Ideas and Information?*, 15 FORDHAM INT'L L.J. 808, 838 (1992)). Senator Mathias cited 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.* at 6550 (quoted in Chin, at 1891, n. 44).

[63] 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." *Id.* at 6551.

exportation to any country."[64] The House report accompanying the 1988 amendment explained: "[T]he principle that no prohibitions should exist on imports to the United States of ideas and information if their circulation is protected by the First Amendment. That principle applies with equal force to the exportation of ideas and information from this country to the rest of the world."[65]

Over the years, the entity charged with administering sanctions under IEEPA, the Treasury Department's Office of Foreign Asset Control, interpreted the informational materials exception narrowly.[66] In 1994, Congress clarified that this exception applies to electronic transmissions, thus excluding 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.'"[67] 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, this statute is the principal authority under which a Trump-era Executive Order over information and communications technology and later executive orders targeting TikTok and WeChat were promulgated.

But what were once "sweeping powers over exports, imports, and private financial transactions"[68] granted by IEEPA have now been enlarged further to cover data. The most direct assertion of executive powers over data flows arises through a series of Executive Orders and their implementing regulations across the Trump and Biden Administrations. 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 a "information and communications technology or service[] … *subject to the jurisdiction* or direction of a foreign adversary … poses an unacceptable risk to the national security of the

---

[64] 50 U.S.C. § 1702(b)(3) (creating an exception for "the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds").

[65] H.R. Rep. No. 100-40, Part. 3, at 113 (1987). See also Note, Alicia Faison, *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, 145 (2021)).

[66] Note, Jarred O. Taylor III, *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).

[67] 50 U.S.C. § 1702.

[68] Barry Carter, *International Economic Sanctions: Improving the Haphazard U.S. International Economic Sanctions: Improving the Haphazard U.S. Legal Regime*, 75 CAL. L. REV. 1159, 1164 (1987).

United States," transactions with that service could be banned.[69] Critically, this Order covered not just goods, but services. Despite being titled as a regulation of the "supply chain," it applies broadly to information and communications technologies and services.

President Trump relied on Executive Order 13873 to ban transactions with TikTok and WeChat in August 2020.[70] Over the subsequent months, however, three federal courts enjoined these bans.[71] On January 5, 2021, President Trump again cited Executive Order 13873 to ban transactions with eight other apps offered by Chinese companies.[72]

Then, on the last day of the Trump Administration, the Commerce Department issued draft rules to implement Executive Order 13873, which the Biden Administration later largely adopted.[73] 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."[74] The Rule empowers the Commerce Secretary to block or require mitigation measures for information and communications technology or services provided by persons "subject to the jurisdiction" of a foreign adversary, when, among other things, the service processes sensitive personal data on greater than one million U.S. persons and "poses certain undue or unacceptable risks."[75]

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."[76]

---

[69] Exec. Order No. 13873, *Securing the Information and Communications Technology and Services Supply Chain,* 84 C.F.R. 22689 (May 15, 2019) (emphasis added).

[70] Exec. Order No. 13942, *Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain*, 85 C.F.R. § 48637 (Aug. 6, 2020), *revoked by* Exec. Order No. 14034, *Protecting Americans' Sensitive Data From Foreign Adversaries*, 86 C.F.R. § 31423 (Jun. 9, 2021); Exec. Order No. 13943, *Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain*, 85 C.F.R. § 48641 (Aug. 11, 2020), *revoked by* Exec. Order No. 14034, *Protecting Americans' Sensitive Data From Foreign Adversaries* 86 C.F.R. § 31423 (Jun. 9, 2021)

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

[72] Exec. Order No. 13971, *Addressing the Threat Posed by Applications and Other Software Developed or Controlled by Chinese Companies*, 86 C.F.R. § 1249 (Jan. 8, 2020), *revoked by* Exec. Order No. 14034, *Protecting Americans' Sensitive Data from Foreign Adversaries*, 86 C.F.R. § 31423 (June 9, 2021).

[73] Exec. Order 13, 873, *Securing the Information and Communications Technology and Services Supply Chain*, 15 C.F.R. § 7 (Jan. 19, 2021).

[74] *Id.* at pt. 1.

[75] *Id.* at pt. 7.

[76] Exec. Order No. 14034, *Protecting Americans' Sensitive Data from Foreign Adversaries,* 86 C.F.R. § 31423 (June 9, 2021). *Id.* (emphasis added).

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.[77] In 2018, through the Foreign Investment Risk Review Modernization Act ("FIRRMA"), Congress explicitly directed CFIUS to review investments that gave access to "sensitive personal data of U.S. citizens."[78] 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.[79] In 2020, Beijing Kunlun Company sold Grindr LLC, 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.[80] 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."[81] 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."[82]

In April 2024, Congress passed the "Protecting Americans from Foreign Adversary Controlled Applications Act," in response in particular to concerns over Chinese control over the massively popular app, TikTok. This law effectively bars 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.[83] Control by a foreign adversary is defined to cover situations where foreign persons from the adversary nation own at least 20 percent of the company, directly or indirectly.[84] 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; (2) and which has 100,000,000 monthly active users.[85]

---

[77] Defense Production Act of 1950 (DPA), codified as amended at 50 U.S.C. app. § 2170; 50 U.S.C. app. § 2170(k).

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

[79] *Roumeliotis,* supra note 22.

[80] Jay Peters, *Grindr has been sold by its Chinese owner after the US expressed security concerns,* THE VERGE, Mar. 6, 2020, https://www.theverge.com/2020/3/6/21168079/grindr-sold-chinese-owner-us-cfius-security-concerns-kunlun-lgbtq.

[81] 85 FR 13719 (Mar. 6, 2020); 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.

[82] Exec. Order No. 14083, *Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States*, 87 C.F.R. § 181 (Sep. 20, 2022).

[83] See 15 U.S.C § 9901 (2)(a); 15 U.S.C § 9901 (2)(g); 10 U.S.C. 4872(d)(2). The nations named as foreign adversaries are China, Iran, North Korea, and Russia. 10 U.S.C. 4872(d)(2).

[84] 15 U.S.C § 9901 (2)(g).

[85] Id. Entities that operate a website or application with the primary purposes of product, business, or travel reviews and information are excluded from the definition. Id.

In April 2024, Congress enacted Protecting Americans' Data from Foreign Adversaries Act ("PADFA") as part of the omnibus bill also containing the TikTok Law.[86] 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 information of a United States individual" to a foreign adversary country, or any entity controlled by such a country.[87]

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.[88] Its official Chinese name, the "Golden Shield" vividly captured this intent to protect against foreign intrusion. 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."[89] 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."[90] The Ministry of Public Security initiated the Golden Shield Project in the mid-1990s, "focused on the more immediate task of stemming the virtual flow of unfiltered information into the country."[91] As James Fallows has written, the Chinese "Internet came with choke points built in."[92] The first campaign to "civilize" Chinese cyberspace was launched in 2000 by eight key ministries and governmental agencies with the "Network Civilization Project."[93]

The Great Firewall was "intended to prevent Chinese people from reaching 'every corner of the world.'"[94] At the time, this meant blocking "foreign ideas [from] flooding into

---

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

[87] *See* H.R. 8038 div. E § 2(a) (2024).

[88] 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, 129-35 (2012).

[89] Lorand Laskai, *Nailing Jello to a Wall*, in CONTROL 195 (Jane Golley, Linda Jaivin & Luigi Tomba, eds. 2017)

[90] Laskai, *supra* note 89, at 203. We can see hints of this in the pedantic 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. 25, 2023, https://nypost.com/2023/02/25/china-is-hurting-us-kids-with-tiktok-but-protecting-its-own/.

[91] Emily Quan, *Censorship Sensing: The Capabilities and Implications of China's Great Firewall Under Xi Jinping*, 39 Sigma: J. Pol. & Int'l. Stud. 19 (2022). Laskai, *supra* note 89, at 194.

[92] James Fallow, *"The Connection Has Been Reset"*, THE ATLANTIC, Mar. 2008, https://www.theatlantic.com/magazine/archive/2008/03/the-connection-has-been-reset/306650/.

[93] MICHAEL KEANE, HAIQING YU, ELAINE JING ZHAO AND SUSAN LEONG, CHINA'S DIGITAL PRESENCE IN THE ASIA-PACIFIC: CULTURE, TECHNOLOGY AND PLATFORMS 49 (2021).

[94] *Id.* at 49. KEANE *et al.* at 49. The ironic reference to "every corner of the world" is to the first email sent from China: "Across the Great Wall we can reach every corner of the world." Gao, supra note.

China."[95] But over the last decade, the Great Firewall of China has expanded decisively from worries over intrusion alone to encompass exfiltration. As we will see, this required a substantial revision of the laws and regulation of the internet. 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.

Famous early moves to oust or block U.S. information service providers in China were largely motivated by efforts to control information flows within the country, though they may have had a twin protectionist goal as well.[96] 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.[97]

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.[98] 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….[99]

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

China's first data localization obligation emerged in 2011 when the People's Bank of China issued a circular on protecting individuals' banking and financial information.[100] Financial regulators worldwide have long embraced data localization, partly to ensure

---

[95] KEANE *et al.,* at 49.

[96] KEANE *et al*., at 62.

[97] Min Jiang, *Authoritarian Informationalism: China's Approach to Internet Sovereignty*, 30 SAIS REV. INT'L AFF. 71 (2010) (noting that "Major Internet services like Twitter, Facebook, YouTube, and Blogger are still blocked."); *Wikimedia censorship in mainland China*, WIKIPEDIA, https://en.wikipedia.org/wiki/Wikimedia_censorship_in_mainland_China#:~:text=Since%20April%2023%2C%202019%2C%20the,versions%20cannot%20be%20accessed%20commonly ("Since April 23, 2019, the entire Wikipedia site (*.wikipedia.org) has been completely blocked in mainland China.").

[98] State Council of the People's Republic of China, The Internet in China Information (June 8, 2010) (translation Xinhua). 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."

[99] *Id.*

[100] Yinfa No. 17 [2011], Notice of the People's Bank of China on Protecting Personal Financial Information by Banking Financial Institutions art. 6, http://www.pbc.gov.cn/english/130733/3911512/index.html ("Personal financial information acquired inside China shall be stored, processed and analyzed inside China.").

immediate control over the regulated entity, including ready access to data held by that entity.[101]

The focus on cybersecurity as a critical component of national security became clear in 2014 when President Xi Jinping himself headed the Central Cyber Security and Informatization Leading Group.[102] President Xi observed that "without cybersecurity, there would be no national security, and without informatization, there would be no modernization."[103] Somewhat surprisingly, he simultaneously recognized the importance of cross-border data flows, noting that "network information flows across borders, and information flow leads technology flow, capital flow, and talent flow."[104] Of course, **"**online public opinion guidance" would remain a touchstone of the Chinese government's approach, he declared.[105]

The government followed up with the National Security Law in 2015, which requires the government to "improve network and information security protection capability" and "maintain the state's sovereignty, security, and development interests in the cyberspace."[106] The law introduced a "national security review" of "key technologies and network information technology products and services."[107]

Also, in 2015, the government issued an action plan on big data, recognizing data as a "a fundamental strategic resource for countries."[108] The plan seemed to suggest the view that shepherding data resources might allow competitive advantage: "our country is first in the

---

[101] See Frontier Economics, *The Extent and Impact of Data Localisation* (June 1, 2022), https://assets.publishing.service.gov.uk/media/63a1a2e88fa8f539198d9bb5/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf ("Sector-specific absolute localisation requirements are more prevalent in relation to … the financial sector, where regulators often require local storage to facilitate access for prudential reasons.").

[102] 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/.

[103] Cyberspace Administration of China, *The first meeting of the Central Network Security and Informatization Leading Group was held and Xi Jinping delivered an important speech, Feb. 27, 2014 21:08,* http://www.cac.gov.cn/2014-02/27/c_133148354.htm (cited by Samm Sacks, *China's Cybersecurity Law Takes Effect: What to Expect*, LAWFARE (June 1, 2017, 10:56 AM), https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect).

[104] Matthew Johnson, *China's Grand Strategy for Global Data Dominance,* CGSP Occasional Paper Series No. 2 (Apr. 2023), https://www.hoover.org/sites/default/files/research/docs/Johnson_ChinasGrandStrategy_Web.pdf .

[105] *Id.*

[106] Ngoc Son Bui & Jyh-An Lee, *Comparative Cybersecurity Law in Socialist Asia*, 55 VAND. J. TRANSNAT'L L. 631, 638 (2022); Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, 8 PA. ST. J.L. & INT'L AFF. 50, 109 (2020).

[107] *Id.* at 638-39; China National Security Law Art. 59.

[108] *Outline of Operations to Stimulate the Development of Big Data,* https://chinacopyrightandmedia.wordpress.com/2015/08/31/outline-of-operations-to-stimulate-the-development-of-big-data/.

world in terms of the scale of Internet and mobile Internet users, it has rich data resources and market advantages for application."[109]

The reorientation of the Great Firewall to control outward flows took its contemporary shape the following year.[110] In 2016, the Standing Committee of the Chinese National People's Congress adopted the Cybersecurity Law, which went into force on June 1, 2017. The Cybersecurity Law introduced a category of "Critical Information Infrastructure" operators, which are under special obligations with respect to the data they hold. The law explained the type of information that was to be protected: that which would "cause serious damage to national security, the national economy and public interest if destroyed, functionality is lost or data is leaked."[111] Most importantly, Critical Information Infrastructure operators would face a data localization obligation, such that the personal data and important data they collect or produce must be stored in China, and transferred overseas only after a security assessment.[112] "Critical Information Infrastructure" was left undefined in the statute, though it would include "public communication and information services." The focus on communications platform operators reflects the Chinese government's ongoing concern with social and political stability.[113] Cybersecurity would still be connected with encouraging a "healthy internet environment."[114]

The data localization obligation was "the most controversial provision" of the Cybersecurity Law.[115] 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. On April 11, 2017, the Cyberspace Administration of China published a draft of its proposed Measures for the Security Assessment of Data Transfers for public comment.[116] Rather than narrowing the data localization obligations of the Cybersecurity Law, it expanded them, now to extend to all "Network Operators," not just those that were operating Critical Information Infrastructure. The security assessment consisted in a self-assessment before

---

[109] *Id.*

[110] 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 (2018) ("The Chinese government … planned to require data localization in the Counterterrorism Law but removed the provision from its final draft in December 2015.").

[111] Cybersecurity Law (China), art. 31.

[112] Cybersecurity Law (China), art. 37.

[113] *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); Geoffrey Hoffman, *Cybersecurity Norm-Building and Signaling with China, in* GOVERNING CYBERSPACE: BEHAVIOR, POWER AND DIPLOMACY 187, 189.

[114] See Lee, *supra* note 110, at 91 ("The government has connected cybersecurity to a healthy internet environment in which rumors, vulgarity, and other unhealthy information should be eliminated.").

[115] Gabriela Kennedy & Xiaoyan Zhang, China Passes Cybersecurity Law, 29 INTELL. PROP. & TECH. L.J. 20, 20 (2017) (cited in Lee, *supra* note 110, at 79).

[116] http://www.cac.gov.cn/2017-04/11/c_1120785691.htm. A month later, the Cyberspace Administration of China published the Measures on the Security Review of Network Products and Services (Interim), focusing on security review of network products and services and not on data flows per se. https://chinacopyrightandmedia.wordpress.com/2017/05/02/interim-security-review-measures-for-network-products-and-services/.

transferring critical or personal data abroad. But a government review was mandated depending on the volume or importance of the data transferred.[117] On July 7, 2022, the final approved measures modified the obligations significantly, requiring government approval in the following cases before transferring data abroad: important data, Critical Information Infrastructure operators and data handlers handling the personal information of over 1 million people; data handlers transferring abroad the personal information of more than 100,000 people or the sensitive personal information of more than 10,000 people; and other circumstances specified by the state cybersecurity department.[118] The focus on volume of personal data echoed similar laws across the world. These data export security assessment obligations went into effect on September 1, 2022.[119] The Regulations require that purchases of network products and services undergo security review when they may "influence national security."[120]

The data export security assessment can be met through a security certification from entities designated by the Cyberspace Administration of China. 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.[121] 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.[122] The PIPL also borrows European practice by permitting standard contractual clauses and certification mechanisms for data transfers abroad.[123] In 2023, the Cyberspace Administration of China finalized rules for Standard Contractual Clauses for Cross-border

---

[117] *Id.* at Art. 9.

[118] Outbound Data Transfer Security Assessment Measures, Art. 4 (translation by DigiChina), https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-effective-sept-1-2022/

[119] In 2017, Cyberspace Administration of China elaborated on the Cybersecurity Law by issuing Regulations on the Security Protection of Critical Information Infrastructure. Draft Regulations on the Security Protection of Critical Information Infrastructure https://www.twobirds.com/en/insights/2017/china/draft-regulations-on-critical-information-infrastructure.

[120] Critical Information Infrastructure Security Protection Regulations, Art. 19, https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/.

[121] The first version was published on June 24, 2022, and a second version on December 16, 2022. https://www.wilmerhale.com/insights/client-alerts/20230104-china-updates-specification-on-security-certification-for-crossborder-personal-information-processing-activities.

[122] Amigo L. Xie *et al.*, *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 (noting that an applicant for a certification may include a "China-based entity within [a multi-national corporation] or a Group of Undertakings.").

[123] *Consumer Data Privacy: EU's GDPR vs. China's PIPL*, Bloomberg Law (May 3, 2023), https://pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-eus-gdpr-vs-chinas-pipl/#:~:text=PIPL%20borrows%20many%20concepts%20from,overview%20of%20each%20law's%20provisions; *see also* 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, 31 (2021).

Transfers of Personal Information.[124] These rules provide a template standard contract designed to facilitate cross-border transfer of personal information.

In 2021, China further elaborated the cybersecurity framework through the Data Security Law. Where parts of the PIPL framework borrowed from the GDPR as we have seen, the Data Security Law was "generally seen as a response to the U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act)."[125] 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.[126] Core data is to be given the highest degree of protection. "Important data" is the next-most sensitive level of data, but its scope is left for future elaboration. Where core data is compromised in a manner that "endanger[s] national sovereignty, security, or development interests," the responsible entity can be fined between 2 million yuan and 10 million yuan, and face the suspension or revocation of its license.[127] The Data Security Law embraces the "free flow of data" as long as it occurs in a "lawful and orderly" manner.[128] 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.[129]

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," with immediate

---

[124] Amigo L. Xie, Prudence Pang, Lingjun Zhang, *China Standard Contract that Impacts Transferring Personal Information from China*, July 20, 2023, https://www.klgates.com/China-Standard-Contract-That-Impacts-Transferring-Personal-Information-From-China-7-20-2023#:~:text=Under%20the%20China%20Standard%20Contract%2C%20the%20overseas%20data%20recipient%20is,onward%20transferee%20to%20ensure%20data.

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

[126] Online Data Security Management Regulations (Draft for Comment) (promulgated by the Cyberspace Admin. of China, Nov. 14, 2016), art. 73, *translated in* Rogier Creemers *et al.*, *Translation: Online Data Security Management Regulations (Draft for Comment) - Nov. 2021*, DIGICHINA (Dec. 6, 2021), https://digichina.stanford.edu/work/translation-online-data-security-management-regulations-draft-for-comment-nov-2021/. *See also* Josh Horwitz, *China Drafts New Data Measures Defines "Core Data,"* REUTERS (Sept. 30, 2021), https://www.reuters.com/world/china/china-issues-draft-rule-data-security-industry-telecoms-2021-09-30/.

[127] Data Security Law, art. 45 (China).

[128] Data Security Law, art. 7 (China).

[129] Data Security Law, art, 36 (China).

effect.[130] The Regulations introduced important exceptions to the requirement for a self-assessment or a data security assessment, including for human resources management.[131]

C. 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 Great Firewall of Europe is not motivated by domestic national security concerns, but rather by the protection of the fundamental rights of European Union residents.[132] For the European Union, then, concerns about foreign government surveillance have thus far principally focused on their threat to the data protection rights of European citizens, rather than a threat to the national security of European states. The end-result may, however, make the Great Firewall of the European Union surprisingly as extensive as the Great Firewalls of China and the United States.

The European Union established crossborder data flow restrictions early on, as a means to ensure that its data protection rules could not be readily circumvented by simply doing data processing overseas. Limiting outbound (but not inbound) flows protected against improper data processing of personal information.[133] This was, of course, the opposite of the early Chinese approach, which placed constraints on inbound information flows, but not outbound flows. 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. The national security turn in these laws is relatively recent, at least at the regional level.

---

[130] *China relaxes security review rules for some data exports*, Reuters, Mar. 22, 2024, https://www.reuters.com/technology/cybersecurity/chinas-cyberspace-regulator-issues-rules-facilitate-cross-border-data-flow-2024-03-22/ (noting that the new rules continued an earlier regulatory easing that had been "greeted with relief by foreign and Chinese firms in China that trade outside the country").

[131] The Regulations now exempt: (1) The transfers of personal data of fewer than 100,000 individuals to external recipients cumulatively by data processors, a marked increase from the earlier exemption limit of 10,000 individuals. (2) Transfer of personal information required for the completion of contracts. (3) Transfer of personal information necessary for cross-border human resources management to ensure entities can comply with foreign labor laws; (4) The transfer of personal information for emergencies to prevent mortality; (5) The transfer of non-personal or important data created during international trade, academic collaboration, industry, and marketing; (6) The transfer of data excluded on an applicable "negative list" in pilot free trade zones. Provisions on Promoting and Standardizing Cross-Border Data Flows (Cyberspace Admin. of China), Mar. 22, 2024, https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm; Bingna Guo et al., 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; Lisa M. Ropple et al., *China Finalizes Provisions on Cross-Border Data Transfer*, Jones Day (Mar. 2024), https://www.jonesday.com/en/insights/2024/03/china-finalizes-provisions-on-crossborder-data-transfer.

[132] Pernot-Leplay, *supra* note 106, at 108.

[133] Chander & Schwartz, supra note 42, at 91.

In 2020, 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.[134] As the Court explained, "those clauses are binding on a controller established in the European Union and the recipient of the transfer of personal data established in a third country where they have concluded a contract incorporating those clauses, it is common ground that those clauses are not capable of binding the authorities of that third country, since they are not party to the contract."[135] Instead, transfers could occur only with "the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection" may be required.[136] A "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 in the case of *Data Prot. Comm'r v. Facebook Ir. Ltd. & Maximillian Schrems*.[137] 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.[138] While focused on the United States, the logic of the decision applied to the transfer of personal data to all countries outside the European Union without an adequacy decision.

Various data protection authorities and courts have tested the viability of Transatlantic data flows in the wake of *Schrems II*.[139] The European Data Protection Board offered guidelines to data exporters to engage in "supplementary measures" for data protection beyond those offered in the Standard Contractual Clauses.[140] The German federal data protection authority also explained that Standard Contractual Clauses and Binding Corporate Rules must be strengthened through supplementary measures in order to ensure that data is "adequately protected from the unlimited access of US security agencies."[141] The data protection authority of the German state of Schleswig-Holstein, on the other hand, declared data transfers to the US generally unlawful. Meanwhile, the Conference of German data protection authorities ("DSK") issued a position paper recommending alternate

---

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

[135] Id. at ¶ 125.

[136] Id.

[137] 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).

[138] *Schrems II, supra* note 134, at ¶¶ 60-64.

[139] For the German and Hungarian language research below, I owe a special debt to extraordinary research assistance by Daniel Csigirinszkij.

[140] European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, V 2.0 (Jun. 18, 2021), at 10-25.

[141] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [BfDI] [Federal Authority for Data Protection and Freedom of Information], *Informationsschreiben zur Auswirkung der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems II")*, 87593/2020 (Oct. 8, 2020), at 3.

legitimate interests and practical solutions.[142] Berlin's data protection authority warned that cross-border "transfer" is defined to include storage in the EU with any possible access from outside, for instance encompassing any American or Asian sub-sub-processors with possible remote access to servers for 24/7 administrative purposes.[143] The Berlin data protection authority called on controllers to "immediately end data exports" if no supplemental measures were in place. Citing a legal opinion from U.S. law professor Steven Vladeck, the Berlin authority observed that cloud service providers might pose special risks because of the broad US definition of "electronic communication service providers" under the Electronic Communications Privacy Act.[144] Furthering this point, the Berlin authority issued separate 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 providers "green."[145] The Bavarian data protection authority's post-*Schrems II* guidance, on the other hand, praised Microsoft's compliance efforts, even while Max Schrems himself criticized it.[146] Microsoft has offered localization within what it calls the "EU Data Boundary."[147] Hamburg's data protection authority, the relevant authority for several Big Tech companies, suggested that because contractual agreements cannot protect against state authorities, transfers to non-adequate countries "can therefore no longer happen in the future."[148] It specially noted that China was "far away" from adequacy.[149]

---

[142] Deutsche Aufsichtsbehörden reagieren auf Safe Harbor-Urteil des EuGH, Dr. Datenschutz (2015), https://www.dr-datenschutz.de/deutsche-aufsichtsbehoerden-reagieren-auf-safe-harbor-urteil-des-eugh/. Commentators called this the "victory of common sense over maximal requirements." Id.

[143] Berliner Beauftragte für Datenschutz und Informationsfreiheit [BlnBDI] [Berlin Authority for Data Protection and Freedom of Information], *Datenexporte: Grundlagen zu Datenexporten in Drittländer*, Datenschutz-berlin.de, https://www.datenschutz-berlin.de/themen/unternehmen/datenexporte.

[144] *Id.*; Stephen I. Vladeck, Expert Opinion on the Current State of U.S. Surveillance Law and Authorities (2021), Datenschutzkonferenz, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2022/ 2022-Vladek_Rechtsgutachten_DSK_en.pdf.

[145] BlnBDI, *Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten*, V 2.0, Bewertungsschema Teil 1 (rechtliche Prüfung) (2021), at 4-5, https://www.datenschutz-berlin.de/fileadmin/ user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_ Videokonferenz-Dienste.pdf.

[146] Bayerische Landesamt für Datenschutzaufsicht [BayLDA] [Bavarian State Supervisory Authority for Data Protection], Übermittlung personenbezogener Daten in Drittländer, https://www.lda.bayern.de/de/ thema_uebermittlung_personenbezogener_daten_in_drittlaender.html. BayLDA, Press Release: *Stärkung der Nutzer-Rechte: Microsoft ergänzt Standardvertragsklauseln* (2020), https://lda.bayern.de/media/pm/pm2020_9.pdf. Max Schrems, The Microsoft "Supplementary Measures" Twitter (2020), https://twitter.com/maxschrems.

[147] https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/.

[148] 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* (2020), https://datenschutz-hamburg.de/ pressemitteilungen/2020/07/2020-07-16-eugh-schrems#.

[149] *Id.*

The Hamburg authority also barred state government agencies from using U.S.-based Zoom because of data transfers to the U.S.[150]

The Hamburg and Berlin authorities also conducted a "Coordinated Investigation of International Transfers," asking hundreds of companies (such as mail, hosting, tracking, adtech service providers and internal client or employee data sharers) to report whether they or their processors might be subject to Section 702 of the U.S. Foreign Intelligence Surveillance Act.[151] The Berlin data protection authority noted that such an information request led most companies to voluntarily stop data transfers.[152]

Other cases have focused on the use of various U.S. service providers. 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.[153] However, a state administrative court withdrew the temporary injunction, in favor of the ongoing consideration of the merits of the case.[154] 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 US agencies was overturned in Baden-Württemberg state court.[155] 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 U.S.[156] In response, some practitioners advised that companies either locally imbed all forms of tracking technology or abstain from using them.[157]

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 Analytics unlawful, despite the supplemental measures, as access under

---

[150] Scott Ikeda, *Hamburg DPA Says Zoom Is Not Compliant With GDPR Due to U.S. Data Transfers, No Longer Allowed for State Government Agencies*, CPO, Aug. 26, 2021, https://www.cpomagazine.com/data-protection/hamburg-dpa-says-zoom-is-not-compliant-with-gdpr-due-to-u-s-data-transfers-no-longer-allowed-for-state-government-agencies/

[151] *Id.*

[152] BlnBDI, *supra* 143.

[153] Stefan Krempl, Gericht: Deutsche Webseiten dürfen keine US-Cookies setzen heise online (2021), https://www.heise.de/news/Gericht-Deutsche-Webseiten-duerfen-keine-US-Cookies-setzen-6288818.html

[154] Christine Albert, Hessischer VGH hebt einstweilige Anordnung gegen Hochschule auf juve.de (2022), https://www.juve.de/verfahren/hessischer-vhg-hebt-einstweilige-anordnung-gegen-hochschule-rheinmain-auf/.

[155] Vergabekammer Baden-Württemberg [Baden-Wuerttemberg Public Procurement Chamber], Jul 13, 2022, 1 VK 23/22, Az. 15 Verg 8/22; Oberlandesgericht Karlsruhe [Karlsruhe High State Court], Sep. 7, 2022, 15 Verg 8/22, Az. 1 VK 23/22; Karin Deichmann et al., US-Cloud and DSGVO / OLG overturns decision of the Public Procurement Chamber BW Skwschwarz.de (2022), https://www.skwschwarz.de/en/details/neuer-beschluss-des-olg-karlsruhe.

[156] Landesgericht München [Munich State Court], Jan. 20, 2022, Az. 3 O 17493/20; Niklas Plutte, LG München: Einbindung von Google Fonts ohne Einwilligung Kanzlei Plutte Kanzlei Plutte (2022), https://www.ra-plutte.de/lg- muenchen-dynamische-einbindung-google-web-fonts-ist-dsgvo/.

[157] LG München: Google Fonts sind nicht mehr datenschutzkonform - Onlineportal von IT Management, It-daily.net (2022), https://www.it-daily.net/it-sicherheit/datenschutz-grc/lg-muenchen-google-fonts-sind-nicht-mehr- datenschutzkonform.

FISA was still possible.[158] On February 10, 2022, the French Commission nationale de l'informatique et des libertés, or "CNIL," followed with a similar judgment, also based on a complaint brought by NOYB. The CNIL ruled the use of Google Analytics violates the GDPR because personal data is transferred by Google to the United States.[159]

The Transatlantic Data Privacy Framework seeks to offer a mechanism for transferring data to the U.S. that satisfies European fundamental rights concerns.[160] It commits the U.S. government to various protections to avoid the disproportionate collection of data and provides remedies for any violation.[161] The Framework alleviates the challenges to transferring data to the U.S. or using suppliers subject to U.S. jurisdiction, but it does not eliminate them. First, data flow restrictions based on national security laws in the EU's member states are largely unaffected by the Framework—as the example of Hungary below will show. Second, 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. Third, Maximilian Schrems and others have already brought lawsuits challenging the Framework as a violation of their fundamental rights, and it too might be repudiated in the future, like its two predecessor Transatlantic arrangements.[162]

Furthermore, digital sovereignty concerns will still lead some EU jurisdictions to bar foreign service providers. For example, the draft EU cloud security certification scheme may include a type of immunity from foreign jurisdiction as a requirement for the highest level of certification, with no exception for U.S. providers. The draft of the European Union's Cybersecurity Certification Scheme for Cloud Services demands that such [cloud service providers] "are operated only by companies based in the EU" with their "registered head office

---

[158] Datenschutzbehörde Republik Österreich [Data Protection Authority of Austria], Datenschutzbeschwerde (Art. 77 Abs. 1 DSGVO), Google LLC, D155.027, 2021-0.586.257, Noyb.eu (2020), https://noyb.eu/sites/default/files/2022- 01/E-DSB%20-%20Google%20Analytics_DE_bk.pdf; Caitlin Fennessy, The Austrian Google Analytics decision: The race is on IAPP (2022), https://iapp.org/news/a/the-austrian-google-analytics- decision-the-race-is-on/.

[159] Raphael Arnold, Behörde zeigt Netdoktor.at bei Google Analytics Grenzen auf juve.de (2022), https://www.juve.de/oesterreich/behoerde-zeigt-dorda-mandantin-bei-google-analytics-schranken-auf/; Kirk J. Nahra et al., The French Data Protection Authority Joins the Austrian Data Protection Authority in Ruling that the Use of Google Analytics Violates the GDPR, WilmerHale (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.

[160] President Biden issued an Executive Order to implement the framework. Executive Order On Enhancing Safeguards for United States Signals Intelligence Activities in October 2022.

[161] Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, 2023 O.J. (L 231).

[162] 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; Laura Kayali, *French lawmaker challenges transatlantic data deal before EU court*, POLITICO EU (Sept. 7, 2023), https://www.politico.eu/article/french-lawmaker-challenges-transatlantic-data-deal-before-eu-court/.

and global *headquarters … in a Member State.*""[163] This would "effectively … exclude [cloud service providers] headquartered outside the EU from seeking "the *highest* level of … certification" on the grounds that such providers would not be immune from foreign law.[164]

National security is reserved to each of the member states, and thus a review of each member state national laws would be required to identify any constraints on outbound data flows.[165] I examine here Hungary's laws, which have not received sufficient attention on these issues.

Hungary's laws include striking limits on outward data flows for national security reasons. The law requires data processing for a variety of state services, including most bodies of the executive and judiciary, to be provided by electronic systems located within Hungarian territory, or within the European Economic Area if approved by the relevant national security authority.[166] Similarly, data processing related to critical or fundamental infrastructure for purposes of national or European interests must take place within European territory.[167] Data processing for any state interest or public body requires a determination that it poses no threat to national security.[168] The 2009 CLV Act on the Protection of Classified Data grants government bodies the power to designate classified data for a variety of state interests, which include national security and the protection of sovereignty.[169] The processing of classified data must be necessary for the public interest and requires a security clearance by the national security agency.[170] For foreign residents, any clearance may be conditioned, including by limitations on onward transfers.[171] These rules permit the Hungarian executive branch significant powers to control the export of data that it believes is related to a public interest.

The Hungarian data protection authority's guidance often promotes data localization, at least within Europe. For example, its good practice guide on digital remote education recommends the use of processors established within the European Economic Area.[172]

---

[163] Kenneth Propp, Peter Swire & Josh Fox, *Oceans Apart: The EU and US Cybersecurity Certification Standards for Cloud Services*, EUROPEAN LAW BLOG, June 27, 2023, https://europeanlawblog.eu/2023/06/27/oceans-apart-the-eu-and-us-cybersecurity-certification-standards-for-cloud-services/ (emphasis in original).

[164] *Id.*

[165] Consolidated Version of the Treaty on European Union (TEU), 2008 O.J. 115, art. 4(2) ("national security remains the sole responsibility of each Member State").

[166] 2013 L Act on Information Security of State and Government Bodies, s. 2 § 3(1), 3(3). In an early embrace of the data sovereignty claims popular today, the preamble to this law characterize "electronic data assets" as "a part of the national wealth."

[167] *Id.*, § 3(2).

[168] *Id.*, s. 9 § 18(4).

[169] 2009. évi CLV. törvény a minősített adat védelméről (Act CLV of 2009 on the protection of classified data) (Hung.), §§ 4(1), 5(1).

[170] *Id.*, §§ 10(1)-10(3), 13.

[171] *Id.*

[172] NAIH, *NAIH/2020/7127 Tájékoztató a digitális távoktatás adatvédelmi és adatbiztonsági vonatkozásairól* (2020).

Similarly, it recommends forgoing the use of certain internet analysis tools due to most providers' processing taking place outside of the EU.[173]

D. The Emerging Doctrine of Immunity from Foreign Jurisdiction

In each of 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 phenomenon 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

Countries now only demand only that data 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.

The reasonable assumption underling 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.[174] The difficulty is that despite the best efforts of the corporation to aspire to global citizenship or official neutrality, 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[175] 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 operations, but not foreign companies with local operations, they may depend on some implicit understanding of the relationship between the parent and subsidiary.

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

---

[173] NAIH, *A Nemzeti Adatvédelmi és Információszabadság Hatóság közleménye a DNS-elemző szolgáltatások igénybevételének veszélyeiről* (2019).

[174] Brad Smith, *The need for a Digital Geneva Convention,* Feb. 14, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/; Kristen Eichensehr, *Digital Switzerlands*, 167 U. PENN. L. REV. 665 (2019).

[175] See, e.g., the French secure cloud standard, which specifies that "the 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. Agence Nationale de la Sécurité des Systèmes d'Information, *supra* note 9, at art. 19.6.b.

States, the Electronic Communications Privacy Act ("ECPA") functions as a "blocking statute," at least with respect to foreign government demands for the contents of U.S. communications.[176] The ECPA permits electronic communication providers to provide information to government entities based on a subpoena or warrant[177]—but only to U.S. government entities.[178] In the European Union, *Schrems II*'s interpretation of European fundamental rights limits foreign government access to data.[179] The Chinese Data Security Law also includes a blocking provision—barring "domestic organizations and individuals" from transferring data stored in China to "foreign justice or law enforcement bodies without the permission of the competent organs of the PRC."[180]

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 depends on the possibility that such a company might follow that home country demand even if it violates local law. 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."[181] 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 to such transfer.[182] When imposed as a requirement for handling personal data, immunity from foreign

---

[176] Aldert Gidari, *The Cross-Border Data Fix: It's Not So Simple*, Center for Internet and Society, Stanford Law School (Jun. 16, 2017), at https://cyberlaw.stanford.edu/blog/2017/06/cross-border-data-fix-it%E2%80%99s-not-so-simple ("[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."); Cong. Res. Serv., *Cross-Border Data Sharing Under the CLOUD Act* ("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."); Richard Salgado, Data Stored Abroad Hearing, https://judiciary.house.gov/wp-content/uploads/2017/06/Salgado-Testimony.pdf ("ECPA includes a broad, so-called 'blocking' provision that restricts the circumstances under which U.S. service providers may disclose the content of users' communications to foreign governments.").

[177] ECPA, 18 U.S.C. 2702(a)(3).

[178] ECPA Section 2711(4) ("the term 'governmental entity' means a department or agency of the United States or any State or political subdivision thereof"). Kate Westmoreland, *The Global Corporate Citizen: Responding to International Law Enforcement Requests for Online User Data*, Harvard JOLT (Aug. 15, 2015), https://jolt.law.harvard.edu/digest/the-global-corporate-citizen-responding-to-international-law-enforcement-requests-for-online-user-data. ("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."").

[179] Case C-311/18, *Data Prot. Comm'r v. Facebook Ireland Ltd.,* ECLI:EU:C:2020:559 (Jul. 16, 2020), para. 185 ("the 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").

[180] Data Security Law, art, 36.

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

[182] 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.

jurisdiction seeks to provide assurance that that data will not be commandeered by a foreign government for its own purposes.

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.[183] Corporations, on the other hand, often institute significant controls over their networks to monitor data flows and prohibit large scale data transfers.[184]

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.[185] Is one company's capital raising in a foreign jurisdiction sufficient to give that jurisdiction leverage over that company, sufficient to demand it to betray another country's citizenry? To take a specific example, is Tencent's minority investment in U.S.-based Epic Games, mean that Epic's blockbuster game Fortnite is 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.[186] All are concerned in various ways with the actions of foreign governments. However, the latter doctrines are in different ways possible defenses that a party can use from a lawsuit in U.S. (and possibly foreign) courts. 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 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.[187]

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. While the traditional doctrines in various ways *privilege* foreign

---

[183] 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).

[184] Erie & Streinz, *supra* note 123, 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 generally* Angelina Fisher & Thomas Streinz*, Confronting Data Inequality,* 60 COLUM. J. TRANSNAT'L L. 829, 867-870 (2022).

[185] 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).

[186] W.S. Kirkpatrick & Co., Inc. v. Environmental Tectonics Corp., International, 493 U.S. 400, 406 (1990).

[187] Jane Lee, *Vitamin "C" Is for Compulsion: Delimiting the Foreign Sovereign Compulsion Defense*, 50 VA. J. INT'L L. 757, 758 (2010).

government actions even in domestic proceedings, immunity from foreign jurisdiction is a way 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. The next Part argues that seeking to wall off a nation through mechanisms such as a requirement of immunity from foreign jurisdiction may prove counterproductive.

II. CASE STUDIES

A review of a handful of recent transnational flashpoints involving the internet demonstrates the extent of the national security internet. They show the national security internet in operation, revealing both its motivations and its costs.

A. TikTok

[to be revised after the S.Ct. decision][188]

Perhaps the most extensive effort to reduce risks of foreign surveillance or manipulation was the plan offered by TikTok in the United States. TikTok's plan combined data localization, a local data trustee, and reincorporation, but it went further yet. ByteDance and TikTok spent years negotiating this plan with CFIUS, seeking to limit the possibility that ByteDance could commandeer TikTok's data or influence its algorithms at the Chinese government's command. TikTok labeled its mitigation plans, set forth in a draft National Security Agreement that ran almost a hundred-pages long, "Project Texas,"[189] invoking the location of the headquarters of its new U.S. technology partner, Oracle.[190]

Under TikTok's "Project Texas," TikTok, Inc., already a California company, was splintered into two companies, the original company, and a new company, TikTok U.S. Data Security Ltd. (TikTok USDS), a new U.S. entity.[191] TikTok USDS would be an "entirely independent business entity" that would be 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.[192] Crucially, its board of directors would be approved by the U.S.

---

[188] The author led the submission of two amicus briefs in the case: https://storage.courtlistener.com/recap/gov.uscourts.cadc.40861/gov.uscourts.cadc.40861.2062101.0.pdf and https://www.supremecourt.gov/DocketPDF/24/24-656/336147/20241227162927329_No.%2024-656%20Amicus%20Brief.pdf.

[189] ByteDance Ltd., TikTok Ltd., TikTok Inc., TikTok U.S. Data Security Inc. & CFIUS Monitoring Agencies, Draft National Security Agreement §§11.5, 11.8-.10 (Parties' Draft as of 8/23/22).

[190] TikTok is engaged in a similar effort in Europe, under the name "Project Clover," with plans that revolve around operations in Ireland. Theo Bertram, *Setting a new standard in European data security with Project Clover*, TIKTOK (Mar. 8, 2023), https://newsroom.tiktok.com/en-eu/setting-a-new-standard-in-european-data-security-with-project-clover.

[191] Matt Perault & Samm Sacks, *Project Texas: The Details of TikTok's Plan to Remain Operational in the United States*, LAWFARE, Jan. 26, 2023, 8:01 AM, https://www.lawfaremedia.org/article/project-texas-the-details-of-tiktok-s-plan-to-remain-operational-in-the-united-states.

[192] National Security Agreement, Articles 2, 3, 8, and 11; Perault & Sacks, *supra* note 272.

government.[193] As the *Washington Post* described, under Project "the Chinese company would cede authority over TikTok's U.S. operations to a three-person board whose members CFIUS would essentially select."[194] Further, TikTok Inc. would have to ensure that the chair of the TikTok USDS would be present at all meetings of the TikTok Inc. board of directors.[195]

Private data of U.S. persons would be stored only on Oracle's servers in the United States.[196] TikTok's software, including its recommendation algorithm, would be deployed through Oracle's infrastructure and reviewed by Oracle and another CFIUS-approved third party.[197] TikTok's content moderation—both human and algorithmic—would be subject to third-party verification and monitoring.[198] The new company's officers would have "extensive national security experience" and would be "Resident Sole U.S. Citizens," citizens of the United States who reside in the United States and who do not hold another citizenship.[199] They would "have, or [be] eligible for, a U.S. personnel security clearance"[200]—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 the national security commitments.[201]

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.

B. "Delete America"

In 2022, the Chinese government issued directive, Document 79, mandating state-owned enterprises in key sectors like "finance, energy, and other" to replace foreign software with home-grown alternatives. The document is apparently so sensitive that high-ranking officials and executives were not given a copy of the document but only allowed to see it. [202] The directive is better known as "Delete A," a reference to "Delete America," as it is largely U.S. software that must be replaced, including likely companies such as Microsoft and

---

[193] National Security Agreement § 3.1.

[194] Drew Harwell, *TikTok and U.S. rekindle negotiations, boosting app's hopes for survival*, WASH. POST, Sept. 15, 2023, https://www.washingtonpost.com/technology/2023/09/15/tiktok-ban-us-negotiations/.

[195] National Security Agreement § 4.3(2).

[196] National Security Agreement, § 1.34 ("For avoidance of doubt, the Recommendation Engine shall be contained and deployed from within the TikTok U.S. Platform."); *id.* at § 8.5 ("[TikTok US Data Security] shall ensure that all such [content delivery network] servers utilized for the (i) delivery of content in the United States reside exclusively in the United States.").

[197] National Security Agreement § 8.4 and Article 9.

[198] National Security Agreement §§ 5.4, 9.13, 16.6.

[199] National Security Agreement § 3.1.

[200] National Security Agreement § 3.1.

[201] National Security Agreement § 21.3 ("Temporary Stop"); § 21.5 ("Suspension of Service").

[202] Liza Lin, *China Intensifies Push to 'Delete America' From Its Technology*, WALL ST. J., Mar. 7, 2024, https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f.

Oracle.[203] The Chinese substitutes are sometimes not as good as their foreign alternatives.[204] 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 U.S. and China. While the replacement of foreign chips in Huawei phones has received a great deal of attention, the replacement of foreign software across key public sector operations in China will likely have greater significance for U.S. exports. Foreign software—because it emanates from a foreign enterprise regulated by a foreign government—simply cannot be secure or trustworthy, according to this approach.

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

C. "Rip and Replace"

The U.S. government, too, is undergoing a massive "rip and replace" process. But unlike the Chinese focus on foreign software, the U.S. program is ripping out Chinese hardware. The process began in 2019 with a focus on telecommunications but has expanded steadily. The Federal Communications Commission (FCC) launched the Secure and Trusted Communications Networks Reimbursement Program in 2019, a program that came to be known as "rip and replace."[205] 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."[206] While the FCC estimated that the program would cost $2 billion, the FCC revised its costs to $5 billion.[207]

Programs to rip and replace now extend beyond telecommunications equipment, and cover such things as drones built by DJI or Autel Robotics and port cranes built by Chinese state-owned company ZPMC.

In 2020, the U.S. Department of Interior banned procurement by its agencies of drones made by China. It lifted its prohibition on nonemergency use "after determining that the potential security risks of these uses were sufficiently low."[208] Reviewing these drone restrictions in 2024, the Government Accountability Office (GAO) concluded that the Bureau

---

[203] *Id.*

[204] Liza Lin, *China Intensifies Push to 'Delete America' From Its Technology*, WALL ST. J., Mar. 7, 2024, https://www.wsj.com/world/china/china-technology-software-delete-america-2b8ea89f.

[205] [Need cite to support proposition] Oversight of the Federal Communications Commission: Hearing Before the United State Committee on Commerce, Science, and Transportation, S. Hrg. 116-589 (Statement of Ajit Pai, Chairman, Federal Communications Commission) (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," according to then-FCC Chairperson Ajit Pai).

[206] https://fccprod.servicenowservices.com/scrp?id=scrp_welcome.

[207] Hill, K. (Dec. 18, 2024). *Rip and Replace Funding Passes as Part of Defense Bill.* PCR Wireless News. https://www.rcrwireless.com/20241218/policy/rip-and-replace-funding.

[208] Gov't Accountability Office, https://www.gao.gov/assets/gao-24-106924.pdf.

of Land Management and the National Parks Service "do not have enough drones for their operations to manage or prevent wildland fires and have shifted some operations to riskier, more costly methods, such as helicopters." "[C]rewed aircraft or ground-based methods may have lost the data quality, safety, and other advantages of drones," the GAO concluded. At the Interior Department, the ban on foreign-made drones has resulted in a "loss of opportunities to collect data on landscape, natural and cultural resources, wildlife and infrastructure," according to the GAO.[209] A farmer reports: "The U.S. drones are not as good as DJI ones but cost twice as much."[210]

Giant cranes at U.S. ports may be the new "Trojan horse," U.S. officials worry.[211] Cranes built by Chinese state-owned enterprise ZPMC "may be controlled, serviced and programmed from remote locations," according to Rear Adm. John Vann, who leads the Coast Guard cyber command. Then Chairman of ZPMC explained in 2018 that information flows help the firm to prevent malfunctions: "Through our main office in Shanghai, you can monitor all the cranes" to help troubleshoot. ZPMC cranes have been deployed in the U.S. for two decades, offering "what industry executives described as good-quality cranes that were significantly cheaper than Western suppliers."[212] The U.S. government will spend more than $20 billion in port security, including domestic cargo-crane production, over the next five years. A U.S. subsidiary of the Japanese company Mitsui will produce cranes in the U.S., "the first time in 30 years that they would be built domestically."[213] 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 U.S. and China.[214]

D. Microsoft Office 365

[to come]

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

---

[209] https://apnews.com/article/china-drones-dji-ban-congress-national-security-09a36a619d2d8a5bd15bb9452774b62c.

[210]

[211] Aruna Viswanatha et al., https://www.wsj.com/politics/national-security/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade?mod=article_inline.

[212] Aruna Viswanatha et al., supra note __.

[213] https://www.wsj.com/politics/national-security/u-s-to-invest-billions-to-replace-china-made-cranes-at-nations-ports-d451ef8f.

[214] https://www.wsj.com/politics/national-security/u-s-to-invest-billions-to-replace-china-made-cranes-at-nations-ports-d451ef8f (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").

manufactured or supplied by persons in China.[215] Modern cars have been described as "smartphones on wheels," and thus "potential spying machines."[216] 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.[217] 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."[218] The rule thus effectively bars the sale of Chinese cars in the U.S., 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.

The Chinese auto industry association has complained that the rule is designed to prop up American manufacturers rather than enhance national security.[219] 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.[220] Commenting on the draft rule, the South Korean government suggested that parts that carried minimal risk be excluded from the rule and noted that the rule would "increase[] costs for the automotive industry and place an undue burden on consumers." [221]

Waymo, the Alphabet subsidiary that is the leading U.S. self-driving car company in the U.S., wrote to the U.S. government to suggest that the National Highway Traffic Safety Administration's Cybersecurity Best Practices for the Safety of Modern Vehicles, and corresponding standards and best practices, "sufficiently provid[e] state of the art security" for

---

[215] https://www.federalregister.gov/documents/2025/01/16/2025-00592/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles. The law also technically covers Russia, but because Russia does not current prospects of being a significant car exporter to the United States, various accounts of the rule describe it as focused on China. 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, *supra* note 69.

[216] https://www.nytimes.com/2024/04/30/technology/regulators-investigate-carmakers-driver-tracking.html.

[217] James Andrew Lewis, *Connected Cars and Spying*, CTR. FOR STRATEGIC & INT'L STUD. (Jan. 10, 2025, 3:46 PM), https://www.csis.org/analysis/connected-cars-and-spying.

[218] *Id.* at 79088.

[219] *US proposed ban on Chinese connected vehicles 'may backfire'*, Global Times (Jan. 11, 2025, 2:57 PM), https://www.globaltimes.cn/page/202501/1326662.shtml; Huaxia, *China firmly opposes U.S. proposed ban on Chinese connected vehicles*, XINHUA (Jan. 11, 2025, 1:36 PM), https://english.news.cn/20240925/2ee14009551f451d8b98fbbed04176e9/c.html.

[220] David Shepardson, *Mexico warns US ban on Chinese car tech could hurt automotive industry*, REUTERS (Jan. 11, 2025, 4:18 PM), https://www.reuters.com/business/autos-transportation/mexico-raises-concerns-about-us-plan-bar-chinese-vehicle-software-hardware-2024-10-28/.

[221] 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, Federal Register Docket No.: BIS-2024-0005, April 30, 2024.

information and communications technology systems in connected vehicles.[222] 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." The group argued that "Any policy that would restrict critical inputs risks setting the overall AV industry back in the US…" Ford too sought to limit the rule only to those systems that "genuinely pose the highest potential national security risks."[223] 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."[224] Ford warned that an overbroad rule would "disrupt U.S. global automotive supply chains."[225]

The connected vehicle rule makes it harder for Americans to get electric vehicles, thus potentially accelerating climate change.[226]

Banning foreign cars or car parts from a market does not guarantee security. Volkswagen recently suffered a major data breach when it left several terabytes of unencrypted information gathered from its European cars, including their locations, publicly available on Amazon cloud servers.[227]

III. WEAKNESSES IN DIGITAL BERLIN WALLS

This Part argues that Digital Berlin Walls might prove both costly to maintain and relatively easy to evade. Sections A through E below summarize these concerns. As the final section shows, national digital security firewalls also carry another, more insidious, risk, not of futility, but rather the rise of another danger: significantly increased control of the domestic information space by the government. 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. Proves Ineffective: Hacking, Spying, and Buying Data

Focusing national security efforts on issues of foreign sovereign compulsion based on ownership can distract from other ways that governments gather data. After all, foreign

---

[222] Waymo, Advance Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, Docket No. 240227–0060, RIN 0694–AJ56, April 30, 2024.

[223] Ford, Advance Notice of Proposed Rulemaking on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, Apr. 30, 2024.

[224] *Id.*

[225] *Id.*

[226] Jim Tankersley, *Biden Doesn't Want You Buying an E.V. From China. Here's Why*, N.Y. TIMES, https://www.nytimes.com/2024/05/27/business/biden-evs.html (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").

[227] Patrick Beuth, Flüpke, Max Hoppenstedt, Michael Kreil, Marcel Rosenbach & Rina Wilkin, *Massive Data Breach at VW Raises Questions about Vehicle Privacy*, SPIEGEL INT'L (Jan. 11, 2025, 11:36 AM), 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.

intelligence services do not rely only on companies within their jurisdiction to obtain information. They often do not rest on their lawful powers at all. They often turn to two extra-legal tools: hacking and spying. They also can employ another tool that may or not be legal—simply purchasing the data from data brokers.[228] 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.[229] Malicious foreign actors hardly need to own services in the U.S. 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. First, consider the hacking of U.S. federal employee records. The U.S. Office of Personnel Management (OPM) "repels 10 million attempted digital intrusions per month,"[230] but it failed to catch a massive hack that transferred millions of federal employee records to a foreign entity.[231] These records apparently included fingerprints and background checks on individuals seeking security clearance.[232] The government had not protected the OPM database with dual-factor authentication, and a government security contractor with access to the OPM database had its security credentials stolen, permitting access to the database.[233] While the U.S. government did not attribute the strike to any foreign actor, others have pointed the finger at China.[234]

Second, beginning as early as 2019, foreign actors infiltrated SolarWinds, a company that provided network monitoring and device management software to the federal government, allowing the hackers access to U.S. government networks.[235] The U.S. government would later "confirm[] the threat actor to be the Russian Foreign Intelligence Service."[236] SolarWinds is a Texas company, with no Russian ownership, but it appears to have been compromised from afar. By infiltrating SolarWinds's monitoring software, the foreign actor could inject its surveillance software into the networks of the US Department of

---

[228] Theodore Rostow, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34 Yale J. on Reg. 667, 669 (2017).

[229] ____ Wired, _____ 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.")

[230] https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[231] 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.").

[232] Josh Fruhlinger, *The OPM hack explained*, CSO, Feb 12, 2020, https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

[233] *Id.*; In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 50 (D.C. Cir. 2019).

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

[235] GOVERNMENT ACCOUNTING OFFICE, FEDERAL RESPONSE TO SOLARWINDS AND MICROSOFT EXCHANGE INCIDENTS (Jan. 2022).

[236] *Id.* (unpaginated page).

Defense, Department of Homeland Security, and the Treasury Department, as well as other federal agencies.[237] Microsoft's President Brad Smith would call it "the largest and most sophisticated attack the world has ever seen."[238]

The third hack involves perhaps one of the most consequential foreign digital interventions. In 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.[239] In this case, as the others, the hackers did not rely on ownership or control over the corporations providing services, but rather infiltration using social engineering and other hacking techniques.[240]

To engage in hacking, governments do not even need to have substantial cybersecurity capacity on their own to obtain information from particular targets. Governments can now buy zero-day exploits from commercial surveillance vendors, who sell spying-as-a-service. These vendors are often based in countries that are political allies of the United States.[241] As a Google Threat Analytics Group report finds, "The government

---

[237] Kim Zetter, *The Untold Story of the Boldest Supply-Chain Hack Ever*, WIRED.COM, May 2, 2023, 6:00 am.

[238] *SolarWinds is 'largest' cyberattack ever, Microsoft president says,* POLITICO, Feb. 15, 2021, https://www.politico.eu/article/solarwinds-largest-cyberattack-ever-microsoft-president-brad-smith/.

[239] Scott 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*, Agence France Press, July 13, 2018, 22:28, https://www.france24.com/en/20180713-death-leaks-russian-hacking-helped-sink-clinton-2016-campaign; Ellen Nakashima and Shane Harris, *How the Russians hacked the DNC and passed its emails to WikiLeaks*, WASH. POST, July 13, 2018 at 7:26 p.m. EDT, https://www.washingtonpost.com/world/national-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.*, *The Tactics and Tropes of the Internet Research Agency* 99 (2019), https://digitalcommons.unl.edu/senatedocs/2. Again, these propaganda efforts did not rely on ownership or control. 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."

[240] A massive hack of AT&T cellular records revealed in July 2024 seems to have utilized vulnerabilities in a U.S.-based cloud security provider. Steve Zurier, *Massive ATT&T breach linked to cloud IT service provider Snowflake,* July 12, 2024, https://www.scmagazine.com/news/massive-att-breach-linked-to-cloud-it-service-provider-snowflake; Joseph Menn & Aaron Gregg, *AT&T says hacker stole call records of 'nearly all' wireless customers* (July 12, 2024, 3:52 p.m.), https://www.washingtonpost.com/business/2024/07/12/att-wireless-hacker-data-breach/.

[241] Google (Threat Analytics Group), Buying Spying: Insights into Commercial Surveillance Vendors 17-20 (Feb. 6, 2024) (identifying commercial surveillance vendors from Greece, Israel, Italy, and Spain); Issie Lapowsky, *Meta calls on the EU to step up fight against spyware*, Feb. 14, 2024, https://www.fastcompany.com/91028657/meta-calls-on-the-eu-to-step-up-the-fight-against-spyware ("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").

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."[242]

But hacking is only one of the tools available to governments. Spying is another. In 2022, a Twitter employee was convicted and sentenced to prison in the United States for spying on behalf of Saudi Arabia.[243] The government charged that he divulged the personal user information of dissidents.[244] Peiter "Mudge" Zatko, Twitter's former head of security, filed a whistleblower complaint with the Securities and Exchange Commission and the Federal Trade Commission in 2022, alleging that foreign countries had pressured Twitter to hire employees chosen by those governments.[245] In 2024, federal authorities arrested a Chinese national working for Google in California for allegedly stealing AI trade secrets to share with a Chinese firm.[246]

The vast collection of personal data by hordes of online companies yields yet another avenue for foreign government access to data: buying the data from brokers. 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."[247] An Executive Order issued in February 2024 seeks to ban some of those sales via data brokers.[248] Congress then adopted similar provisions in the Protecting Americans' Data from Foreign Adversaries Act ("PADFA") as part of the omnibus bill that also enacted the TikTok Law.[249]

Thus, there are multiple alternatives to exfiltrating data—hacking, spying, and buying data—that do not depend on ownership or control of key components of the supply chain.

B. Reduces Competition

One of the greatest harms of immunity from foreign jurisdiction or national firewalls is the reduction in 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

---

[242] *Id.* at 16.

[243] Kevin Collier, *Former Twitter employee sentenced to more than three years in prison for spying for Saudi Arabia*, NBC NEWS, Dec. 14, 2022, 5:13 PM EST, https://www.nbcnews.com/tech/security/former-twitter-employee-sentenced-three-years-prison-spying-saudi-arab-rcna61384.

[244] Kalley Huang and 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.

[245] Joseph Menn, Elizabeth Dwoskin & Cat Zakrzewski, *Former security chief claims Twitter buried 'egregious deficiencies,'* WASH. POST, Aug. 23, 2022, Updated Aug. 23 at 12:27 p.m., https://www.washingtonpost.com/technology/interactive/2022/twitter-whistleblower-sec-spam/.

[246] https://www.nytimes.com/2024/03/06/us/politics/google-engineer-china-ai-theft.html.

[247] Faison, *supra* note 65, at 130.

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

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

economy because they now have fewer providers, which are likely to be able to charge higher prices while providing worse service.[250]

One of the risks of reducing competition is that the suppliers that remain may not have the same cybersecurity protections as the global providers.[251] For example, consider a school district that is told that it cannot use a U.S.-based computer provider because it might transfer data to the United States.[252] This would potentially bar Google Chromebooks, but also Apple's Macbooks and Dell's laptops. If there were concerns about transferring data to China, it might be difficult to approve the purchase of China-based Lenovo's laptops. While there would be some companies that lack operations that are subject to the jurisdiction of disfavored foreign countries, they would be far fewer in number than those that largely operate globally. This loss of choice would impose a heavy burden for consumers, businesses, and government actors—over time reducing the quality while increasing the price of the desired transaction.

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.[253] 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.[254] Reporting suggests that the more permissive interpretation was due in part to "China's fears about its precarious economy" and the perceived need to "keep foreign investors onside."[255]

Economic prosperity is itself a component of national security. Thus, by hampering domestic commerce, national firewalls harm national security, even while seeking to protect it.

C. Expensive to Maintain

[250] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 721 (2015).

[251] Id. at 719 (arguing that "the 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").

[252] This is not theoretical. Various European data authorities have questioned the use of Google Chromebooks in education. See, e.g., *Danish Data Protection Authority requests municipalities using Chromebooks to stop sending unnecessary data to Google,* GIGAZINE, Feb. 09, 2024, 17:50:00, https://gigazine.net/gsc_news/en/20240209-denmark-orders-to-stop-student-data-to-google/.

[253] Tom Hancock, *China Loosens Cross-Border Data Rules to Ease Business Pressure,* Bloomberg (May 22, 2024), https://www.bnnbloomberg.ca/china-loosens-cross-border-data-rules-to-ease-business-pressure-1.2050507.

[254] Stuart Lau, *Deal over dim sum: China caves to EU on data to keep investors sweet*, POLITICO, Nov. 9, 2023, 5:10 AM CET, https://www.politico.eu/article/deal-over-dim-sum-china-caves-eu-data-keep-investors-sweet/.

[255] *Id.*

In addition to the additional economic costs resulting from reduced competition, national firewalls are expensive to maintain. They require public resources for enforcement.[256] 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 comply with U.S. national security demands, and is planning to spend twelve billion euros to do so in Europe as well.[257]

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.

Some will reply that this claim did not prove true for decades, as the United States did not respond to the Great Firewall of China by shutting out Chinese apps. But for the first two decades, the U.S. did not face the prospect of any wildly popular Chinese internet services in the United States. Beginning with TikTok, and extending to consumer retailers Shein and Temu, the U.S. has finally begun to grapple with Chinese companies that are finding success on our shores—and calls for a tit-for-tat response.[258]

Some will note, correctly, that China has already banned U.S.-based information services such as the Facebook, the NY Times, and Wikipedia.[259] But it still has plenty of other possible targets if it chooses to retaliate for U.S. bans of its apps. Indeed, in September 2020, China established an "unreliable entity list" in the wake of the Trump executive orders targeting TikTok and WeChat.[260] This has been described as a "tit for tat" move.[261] When the *Wall Street Journal* reported that the Chinese government was banning government employees

---

[256] Compare the cost of more traditional cybersecurity firewalls to protect specific computers. *See* U.S. Gov't Accountability Off., GAO-16-294, DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System 2 (Jan. 2016) (The U.S. government's firewall, named Einstein, cost $5.7 billion dollars to develop, and it is still only "partially meeting its stated system objectives.")

[257] Kristen Cabrera & Sean Saldana, *Project Texas: Inside TikTok's billion-dollar plan to stay in America*, TEX. STD., Mar. 27, 2023 3:59 pm, https://www.texasstandard.org/stories/project-texas-tiktok-plan-stay-america-oracle-security/; Theo Bertram, *TikTok sets new standards for security and sustainability through €12bn Project Clover programme*, https://newsroom.tiktok.com/en-eu/tiktok-sets-new-standards-for-security-and-sustainability-through-12-bn-project-clover-programme, TikTok, Nov 30, 2023.

[258] 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 (describing threatened bans on TikTok and WeChat as an "overdue response, a tit for tat, in a long battle for the soul of the internet 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"); Liao, supra note —.

[259] 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.

[260] Qingxiu Bu, *China's Blocking Mechanism: The Unreliable Entity List*, 19 J. INT'L TRADE L. & POL'Y 159, 159 (2020).

[261] *Id.* ("On 19 September 2020, MOFCOM Regulation was issued one day after the USA sought to ban Chinese-owned apps WeChat and TikTok. The provisions constitute the basis for more comprehensive tit-for-tat retaliation by the Chinese Government in response to a series of US executive orders and statutory sanctions.") (citation omitted).

from bringing iPhones to government offices, Apple saw nearly a *200 billion dollar* decline in its market capitalization.[262]

With respect to the argument that turnabout is fair play, Justice Brennan offered a sharp riposte: "That the governments which originate this propaganda themselves have no equivalent guarantees only highlights the cherished values of our constitutional framework; it can never justify emulating the practice of restrictive regimes in the name of expediency."[263]

E. Highly Intrusive

Implementing national firewalls and immunity from foreign jurisdiction prove Herculean tasks. 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.

Requiring immunity from foreign jurisdiction becomes a quest with no end. 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. A memo from a U.S. law firm asked to advise the Dutch Ministry about risks of U.S. intelligence services gaining access to that country's citizens' data: "it is advised not to employ US nationals with access to relevant data."[264] 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. 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 shareholders and employees 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.

---

[262] Nicole Goodkind, *Apple lost $200 billion in two days after reports of iPhone ban in China*, CNN, Sept. 7, 2023, updated 4:29 PM EDT, https://www.cnn.com/2023/09/07/investing/apple-stock-iphone-china-ban; Yoko Kubota, *China Bans iPhone Use for Government Officials at Work*, WALL ST. J., updated Sept. 6, 2023 5:47 pm ET, https://www.wsj.com/world/china/china-bans-iphone-use-for-government-officials-at-work-635fe2f8; Dan Gallagher, *Apple Becomes the Biggest U.S.-China Pawn Yet*, WALL ST. J., Updated Sept. 8, 2023 12:01 am ET, https://www.wsj.com/tech/apple-becomes-the-biggest-u-s-china-pawn-yet-ad093256 (describing reports of Chinese government ban as "costing the company about $194 billion in market value). The Chinese government denied the reports. Rachel Liang, *China Says No Laws, Regulations Banning Use of Apple's iPhones,* WALL ST. J., updated Sept. 13, 2023, 5:51 am ET, https://www.wsj.com/tech/china-denies-ban-on-apples-iphones-aca9f2af.

[263] Lamont v. Postmaster General, 381 U.S. 301, 310 (1965) (Brennan, J., concurring).

[264] Gretchen Ramos, Andrea Maciejewski, & Herald Jongen, *Application of the CLOUD Act to EU Entities* (Greenberg Traurig LLP memo July 26, 2022).

And then every vendor's manager, employee and shareholder as well need to be vetted. And the same for the vendors' vendors, ad absurdum.

F. Increases Government Control

The ability to select who can and who cannot provide services that include personal data can be employed for political ends. A government could use the 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 beyond that which the government is willing to tolerate.[265]

To establish the threat posed by TikTok to U.S. national security, the U.S. government pointed to (1) Chinese government "authority and supervision over nominally private … organizations";[266] (2) Chinese laws that require private persons to assist Chinese intelligence services;[267] and (3) Chinese rules that give the government the power "take control of an organization's facilities, which includes communications equipment."[268] The U.S. government was also worried that (4) the Chinese government might compel TikTok to push Chinese Communist propaganda to U.S. residents.

These are, indeed, serious concerns. China's National Intelligence Law does in fact require "[a]ll organizations [to] … assist … national intelligence efforts in accordance with law." 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."[269] But there are reasonable concerns about the effectiveness of such constraints. It is important to note that these rules apply to "[a]ll organizations," not just domestic ones, so that even major U.S. technology companies might fall within the scope of these rules. Thus, even Apple or Microsoft, or at least their Chinese subsidiaries, are subject to China's National Intelligence Law.[270] Microsoft

---

[265] See, e.g., David McCabe, *TikTok Bid Highlights Oracle's Public Embrace of Trump*, N.Y. TIMES (Sept. 4, 2020), https://www.nytimes.com/2020/09/04/technology/oracle-tiktok-trump.html.

[266] Defendants' Memorandum in Opposition to Plaintiffs' Renewed Motion for a Preliminary Injunction against Commerce Department Prohibitions, TikTok Inc. v. Trump, 2020 WL 6883229 (D.D.C.), No. 1:20-CV-2658-CJN (Oct. 23, 2020) ("The PRC exercises authority and supervision over nominally private or non-governmental organizations, including through Party Committees or Corporate CCP Committees at those entities.") (internal quotes omitted).

[267] *Id.* (noting that "in 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 quotes omitted).

[268] *Id.* ("The law expressly permits Chinese intelligence institutions to … take control of an organization's facilities, which includes communications equipment.") (internal quotes omitted).

[269] China National Intelligence Law, art. 8. See also China Data Security Law, art. 35 ("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…").

[270] *See e.g.,* Erie & Streinz, *supra* note 123 (noting how Apple was forced to host Chinese users' iCloud accounts in data centers based in mainland China to comply with Cybersecurity Law.).

is even in the process of moving its artificial intelligence engineers from China anticipating U.S. worries.[271]

In response to these concerns, ByteDance and TikTok negotiated with CFIUS mitigation measures to limit the possibility that ByteDance could commandeer TikTok's data at the Chinese government's command. As we have seen, that mitigation agreement proved insufficient for the U.S. Congress and the Biden Administration, but 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. was splintered into two companies, the original company, and a new company, TikTok U.S. Data Security (TikTok USDS).[272] TikTok USDS would be an "entirely independent business entity" that would be 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.[273] Crucially, its board of directors would be approved by the U.S. government. The *Washington Post* describes Project TikTok as "a sweeping plan ByteDance introduced … under which the Chinese company would cede authority over TikTok's U.S. operations to a three-person board whose members CFIUS would essentially select."[274]

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…"[275] 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.[276]

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."[277] This account of the negotiations thus 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.

---

[271] 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 7:43 am ET, https://www.wsj.com/tech/ai/microsoft-asks-hundreds-of-china-based-ai-staff-to-relocate-amid-u-s-china-tensions-b626ff8c.

[272] Matt Perault & Samm Sacks, *Project Texas: The Details of TikTok's Plan to Remain Operational in the United States*, LAWFARE, Jan. 26, 2023, 8:01 AM, https://www.lawfaremedia.org/article/project-texas-the-details-of-tiktok-s-plan-to-remain-operational-in-the-united-states.

[273] Perault & Sacks, *supra* note 272.

[274] Drew Harwell, *TikTok and U.S. rekindle negotiations, boosting app's hopes for survival*, WASH. POST, Sept. 15, 2023, https://www.washingtonpost.com/technology/2023/09/15/tiktok-ban-us-negotiations/.

[275] Emily Baker-White, *A Draft of TikTok's Plan to Avoid A Ban Gives The U.S. Government Unprecedent Oversight Power,* FORBES (Aug. 21, 2023, 3:39 PM), https://www.forbes.com/sites/emilybaker-white/2023/08/21/draft-tiktok-cfius-agreement/?sh=194955a9112a.

[276] Harwell, *supra* note 274.

[277] Baker-White, *supra* note 275274.

In sum, 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.[278] These include government supervision of private parties and government authority to comandeer the company's equipment and data.[279] 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."[280]

Project Texas would prove insufficient for some U.S. legislators, especially in the wake of the horrific Hamas attack on Israel on October 7, 2023. Supporters of a divest-or-ban bill argued that TikTok was stoking sentiment against the Israeli response in Gaza. Representative Mike Gallagher, one of the two lead sponsors of the law, argued on November 4, 2023 that U.S. youth were siding with the Palestinians over Israel because of TikTok.[281] The House Select Committee on the Chinese Communist Party summarized Representative Gallagher's argument as follows:

> @repgallagher: How are so many young people in America siding with Hamas terrorists? Who have killed at least 30 Americans and kidnapped a dozen more, still at this moment holding 10 hostages. Where are they getting their news? The answer, increasingly, is TikTok - an app under the de facto control of the Chinese Communist Party.

Representative Raja Krishnamoorthi, one of the two lead sponsors of the law, explained that it gained support because of "[the] Oct. 7[, 2023 Hamas terrorist attacks], including the fact that Osama bin Laden's 'Letter to America' went viral on TikTok and the platform continued to show dramatic differences in content relative to other social media platforms."[282] Senator Mitt Romney reported that there "overwhelming support for us to shut down potentially TikTok" because of the volume of "mentions of Palestinians."[283] The Congress targeted a speech app on national security grounds because the app was a hotbed of speech the Congress disliked.

Project Texas and the TikTok Law thus show how powers to block crossborder data flows can be used to assert control over information flows within a country, an idea that China made familiar with its Great Firewall.

---

[278] Harwell, *supra* note 274 (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").

[279] *Id.* ("The law expressly permits Chinese intelligence institutions to … take control of an organization's facilities, which includes communications equipment.") (internal quotes omitted).

[280] Karim Farhat, *TikTok's Project Texas: The wrong template for tomorrow's digital economy*, INTERNET GOVERNANCE PROJECT, Mar. 9, 2023, https://www.internetgovernance.org/2023/03/09/tiktoks-project-texas-the-wrong-template-for-tomorrows-digital-economy/.

[281] https://x.com/committeeonccp/status/1720791984632127715.

[282] Sapna Maheshwari et al., *House Passes Bill to Force TikTok Sale From Chinese Owner or Ban the App*, N.Y. TIMES, March 13, 2024.

[283] Erin Alberty, *Sen. Romney links TikTok ban to pro-Palestinian content*, AXIOS, May 6, 2024, https://www.axios.com/local/salt-lake-city/2024/05/06/senator-romney-antony-blinken-tiktok-ban-israel-palestinian-content.

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 take various measures to protect against government orders compelling the production of personal data. They 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 choose vendors to store and process data and jurisdictions to store and process data 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. Kristen Eichensehr elaborated the concept of "Digital Switzerlands," borrowing a term offered by Microsoft President Brad Smith in 2017.[284] 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 information demands.

This Part surveys and catalogs 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 describes some of the 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, thus, will be part of the corporate toolkit to avoid government data compulsion actions. Another mechanism is encryption, where data held by the company is encrypted to prevent access without the decryption key.

B. Data Localization

Many have described efforts by companies to localize data in order to meet local government demands.[285] For example, Alibaba has built local servers in Vietnam to help companies comply with Vietnamese data localization obligations.[286] Faced with similar demands to localize data in Vietnam, Meta sought to placate the authorities by meeting their demands to censor content instead.[287]

---

[284] Eichensehr, *supra* note 174.

[285] *See, e.g.,* Chander & Le, *supra* note 7; Note, Wenxi Lu, *Data Localization: From China and Beyond*, 31 IND. J. GLOBAL LEGAL STUD. 183 (2024)

[286] Lien Hoang, *Alibaba to Build Vietnam Data Center to Follow Local Storage Law*, Nikkei, May 1, 2024 10:34 JST, https://asia.nikkei.com/Business/Technology/Alibaba-to-build-Vietnam-data-center-to-follow-local-storage-law.

[287] Rebecca Tan, *Facebook helped bring free speech to Vietnam. Now it's helping stifle it.*, June 19, 2023 at 2:00 a.m. EDT, https://www.washingtonpost.com/world/2023/06/19/facebook-meta-vietnam-government-censorship/.

C. Data Trustees

Another strategy of companies is to locate a trusted local partner, through which they continue to offer services. In 2015, 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.[288] Various Microsoft cloud services would be offered by computer servers owned and operated by the German telecommunications giant Deutsche Telekom.[289] 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. But in 2018, the two companies dissolved their partnership due to a combination of high prices and issues with stability, performance, and security.[290] Temu uses a similar model to store U.S.-persons data on Microsoft servers in the United States.[291]

In China, in response to the Chinese Cybersecurity Law described above,[292] Apple adopted a model similar to Microsoft's data trustee arrangement, though that model continues through today and is not optional. Apple localized its Chinese user data on computer servers run by a state-owned Chinese firm.[293] As the *New York Times* reports, "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."[294] Salesforce, too, now

---

[288] *T-systems to act as Data Trustee for Microsoft Cloud in Germany*, DIGITALISATION WORLD (2024), https://digitalisationworld.com/news/46236/t-systems-to-act-as-data-trustee-for-microsoft-cloud-in-germany.

[289] Deutsche Telekom AG, *Deutsche Telekom to act as Data Trustee for Microsoft Cloud in Germany* (2015), https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-to-act-as-data-trustee-for-microsoft-cloud-in-germany-362074.

[290] Jos Poortvliet, *Microsoft and Telekom no longer offer cloud storage under German jurisdiction*, NEXTCLOUD (2024), https://nextcloud.com/blog/microsoft-and-telekom-no-longer-offer-cloud-storage-under-german-jurisdiction/.

[291] Temu's privacy policy states: "Data of Temu U.S. users will be stored by default in the infrastructure of Microsoft Azure or a similar cloud service provider in the U.S. Temu is a global one-stop shopping destination, therefore where necessary, Temu may transfer data related to order fulfillment to service providers in other countries to provide order fulfillment and logistics services. Sensitive personal information (such as account and profile information) unrelated to fulfillment services will not be transferred. At the same time, in all cases, we will ensure that all transfers of personal data comply with applicable U.S. legal requirements." Temu privacy policy, (last visited May 29, 2024) https://www.temu.com/privacy-and-cookie-policy.html?_x_sessn_id=ggr0feko6d&refer_page_name=login&refer_page_id=10013_1717038846807_vmbdwe488q&refer_page_sn=10013

[292] *See supra* notes 110-114 and accompanying text.

[293] Jack Nicas, *et al., Censorship, Surveillance and Profits: A Hard Bargain for Apple in China,* https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html.

[294] *Id.*

"relies on a local partner to operate some of its products and services there, effectively isolating its China business from its global operations."[295]

D. Reincorporation (or "Anywhere-But-China" ("ABC"))

Recognizing that their national origins might make them unwelcome elsewhere, some companies are reincorporating to neutral jurisdictions. Chinese firms, in particular, must "grapple with a kneejerk presumption from foreign governments of their fealty to the Chinese Communist Party."[296] Some have adopted an effort to refashion themselves as from "Anywhere-But-China" ("ABC").

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.[297] Shein's CEO even described its company as "essentially American," a remark that Shein then worried would raise trouble in China, which remains a critical part of its supply chain.[298] Indeed, "the model of "de-Chinafying" to gain business success... raises questions of loyalty to China that some in Beijing find uncomfortable."[299] Temu, the successful goods e-commerce company, says that it "was founded in Boston, Massachusetts in 2022," even though it is owned by Chinese e-commerce giant Pinduoduo.[300] 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.

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

---

[295] Elaine Yu Follow & Yoko Kubota, *Companies Try New Strategy to Stay in China: Siloing*, WALL ST. J., June 25, 2023 12:01 am ET, https://www.wsj.com/articles/companies-try-new-strategy-to-stay-in-china-siloing-61c88721?mod=article_inline.

[296] Sarah Zheng, *Temu and* While Shein was "born in China," it reincorporated in Singapore in 2022 to assuage national security concerns of the countries in which it operates. 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; *Keep Trying to Shed Their Chinese Roots*, BLOOMBERG, July 16, 2024, https://www.bloomberg.com/news/newsletters/2024-07-16/temu-and-shein-keep-trying-to-shed-their-chinese-roots.

[297] 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

[298] 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.

[299] *Id.*

[300] 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.

requests from their home jurisdiction's governments. 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.[301] 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.[302] Twitter unsuccessfully sought to publicly disclose more detailed information about the national security letters it received from the U.S. government.[303]

The most famous such incident was Apple's refusal to cooperate with the Federal Bureau of Investigation (FBI) demand to help break into the iPhone of those responsible for a horrific terrorist attack in San Bernardino, California. 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.[304] Apple challenged the order, citing its policy agreement with its customers not to undermine the security of its devices.[305] The issue was resolved when the Department of Justice announced that it had unlocked the iPhone through alternative channels.[306]

Neil Richards and Woody Hartzog rightly note that Apple and Microsoft fought these battles with U.S. law enforcement "to earn and keep the trust of their customers."[307] We might go further to note that the companies sought to assure not only their customers, but also foreign governments. Foreign governments, too, were the audience of these efforts. These moves 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, and perhaps even in a case involving terrorism.

F. Limits of Corporate Measures

However, corporate efforts can only go so far. Even if the data is encrypted many services depend on the company holding the encryption key, so that it can usefully process

---

[301] Gonzales v. Google, Inc., 234 F.R.D. 674, 679 (N.D. Cal. 2006) ("The subpoena … required the companies to produce the text of users' search queries."). Even this case demonstrates that companies will make different calculations at different times. As the court notes in that case, the other companies that received the same subpoena seem to have complied. Id. ("AOL, Yahoo, and Microsoft appear to be producing data pursuant to the Government's request.").

[302] United States v. Microsoft Corp., 584 U.S. ___, 138 S. Ct. 1186 (2018).

[303] Twitter v. Garland, 61 F.4th 686 (9th Cir. 2023).

[304] Dustin Volz, Mark Hosenball, *FBI director says investigators unable to unlock San Bernardino shooter's phone content*, REUTERS, Feb. 9, 2016, https://www.reuters.com/article/us-california-shooting-encryption-idUSKCN0VI22A/; Andrew Blankstein, *Judge Forces Apple to Help Unlock San Bernardino Shooter iPhone*, NBC, Feb. 16, 2016, https://www.nbcnews.com/storyline/san-bernardino-shooting/judge-forces-apple-help-unlock-san-bernardino-shooter-iphone-n519701.

[305] Id.

[306] Id.

[307] Neil Richards & Woody Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1185 (2017).

the information on behalf of the data subject or for purposes such as advertising.[308] This means that a government could conceivably compel that company to decrypt and turn over the data. If the company holds the encryption key, it can be asked to use it. End-to-end encryption could render information unreadable even by the service provider, but it would interfere with content moderation, fraud detection, search services and spam filtering, as such features often require the service system to identify keywords or patterns within the data content.[309] This also impacts companies' abilities to collect data to run targeted ads, affecting the profitability of adopting such technologies.[310]

Data localization and data trustees may not be enough if the local government is not convinced that it renders 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.[311] 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 to an array of commitments including running services exclusively from the data trustee's infrastructure and carefully controlled access to that protection information, failed to satisfy the U.S. Congress or the Biden Administration, resulting in a law requiring either divestiture or ban.[312]

G. Exit

When efforts to satisfy governments fails, some corporations simply exit. Albert Hirschman's famous typology – exit, voice, loyalty--describes options for individuals with grievances with organizations.[313] For corporations, like individuals, exit is a costly option. For corporations, 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.

A Pure Theory of Local Expenditures

Author(s): Charles M. Tiebout

Source: The Journal of Political Economy, Vol. 64, No. 5, (Oct., 1956), pp. 416-424

---

[308] Timothy B. Lee, *NSA-proof Encryption Exists. Why Doesn't Anyone Use It?*, WASH. POST (June 13, 2013), https://www.washingtonpost.com/news/wonk/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/.

[309] Id.

[310] *Id.*

[311] See supra notes 143-146 and accompanying text.

[312] Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (2020) (IEEPA executive order banning transactions with TikTok); *Presidential Order Regarding the Acquisition of Musical.ly by ByteDance Ltd.*, 85 Fed. Reg. 51297 (Aug. 14, 2020) (CFIUS-based executive order requiring divestment); Protecting Americans from Foreign Adversary Controlled Applications Act, *supra* note 6.

[313] ALBERT O. HIRSCHMANN, EXIT, VOICE, LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1970).

The Tiebout model sees exit as a means of expressing consumer discontent

Google famously left China,

But exit might not be voluntary. Host countries can kick out foreign corporations, and home countries can require their corporations to leave

So such exclusion zones come in three varieties: leaving a country voluntarily, being kicked out, being told by its home government to stay out of a foreign country.

V. SOLUTIONS

A central impetus for the rise of the national security internet, with border controls for exiting data through mechanisms such as data localization and a requirement for immunity from foreign jurisdiction, is concerns over foreign surveillance.[314] Unilateral corporate responses may fail to satisfy governments, which may be reluctant to lower their Digital Berlin 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 rendering those border controls less necessary.

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 governing their own foreign surveillance activities.

---

[314] 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 by the U.S. to Russian hackers) demonstrate. *See supra* notes 235 - 238 and accompanying text; https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack; *With Stuxnet, Did The U.S. And Israel Create a New Cyberwar Era?*, WIRED, Jan. 16, 2011, https://www.wired.com/2011/01/with-stuxnet-did-the-u-s-and-israel-create-a-new-cyberwar-era/; Cybersecurity and Infrastructure Security Agency, *Indicators Associated With WannaCry Ransomware,* June 07, 2018, https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware; Dept. of Justice, Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace, Oct. 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and. Governments have responded to by seeking to make their critical digital infrastructure more secure. *See, e.g.,* The Network and Information Security (NIS2) Directive, 2022/2555 of the European Parliament and of the Council of 14 December 2022.

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.[315] This is one way to understand *Schrems II*'s interpretation of European fundamental rights limiting foreign government access to data.[316]

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 it is being processed.[317] As Woodrow Hartzog and Daniel Solove write, "Poor privacy will undermine even the best data security."[318] 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."[319] 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 whether brokers can legally sell the data they collect.

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 the 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

This section argues that 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. The U.S. can lead the way, modeling limitations on foreign mass surveillance (including reform of the Foreign Intelligence Surveillance Act) and providing remedies for violations.[320]

There is precedent for governments revising their own surveillance rules to reduce the concerns of foreigners. The principal precedent is U.S. efforts to obtain adequacy under the terms of European Union data protection law. While the original Safe Harbor facilitating data flows to the United States did not involve any U.S. commitments regarding surveillance

---

[315] *See supra* notes 176-180 and accompanying text.

[316] *See supra* notes 179 and accompanying text

[317] Faison, *supra* note 65, at 140 (arguing for a national comprehensive privacy law need 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").

[318] WOODROW HARTZOG & DANIEL SOLOVE, BREACHED 142 (2022).

[319] *Id.* at 146.

[320] *See generally* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 343-354 (2015).

or other law enforcement access to data,[321] the U.S. has made commitments regarding foreign surveillance of EU persons' data subsequent to *Schrems I* and *Schrems II*. The EU-US Data Privacy Framework offers the latest version of the U.S. commitments to protect EU data in the context of national intelligence.[322] 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.[323] 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."[324] 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 application for review."[325] Unlike the Safe Harbor and the Privacy Shield which name the European Union as the sole beneficiaries of those arrangements,[326] the U.S. orders implementing the Data Privacy Framework are written to be expandable beyond the European Union.

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.[327] Section 702's procedures are designed largely to protect the information of U.S. persons that might be incidentally collected in this process. Indeed, even many reform proposals seek to better protect U.S. persons from being caught up in such surveillance,[328] neglecting concerns of foreign persons

---

[321] Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666 (Jul. 24, 2000), https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission.

[322] Enhancing Safeguards for United States Signals Intelligence Activities, Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 7, 2022); see also https://www.dataprivacyframework.gov/.

[323] Exec. Order 14,086, at § 2.

[324] Exec. Order 14,086, at § 3.

[325] Exec. Order 14,086, at § 3.

[326] *See, e.g., Issuance of Safe Harbor Principles and Transmission to European Commission*, 65 Fed. Reg. at 45666 (Jul 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 Shield 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.").

[327] 50 U.S.C. § 1881a (referred to here by its popular name, "Section 702"). See American Civil Liberties Union, Warrantless Surveillance Under Section 702 of FISA, https://www.aclu.org/issues/national-security/warrantless-surveillance-under-section-702-fisa. 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 focused largely on protecting U.S. persons).

[328] *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,

in the process. The Data Privacy Framework's limits on foreign surveillance described above should be incorporated into Section 702. 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. Section 702 has a sunset provision, and expires if not reauthorized by April 2026.[329] Assuming that Section 702 is reauthorized, one approach to 702 reform might be to enshrine the constraints on foreign intelligence found in Executive Order 14086 into the reauthorized law.[330] This executive order implements the Data Privacy Framework by limiting surveillance with necessity and proportionality requirements, banning surveillance to suppress criticism, dissent or silence individuals, or seek an advantage for U.S. corporations.[331]

Again, in an effort to obtain an adequacy ruling from the European Commission, Japan, too, provided additional protections against surveillance and law enforcement access to data. As the European Commission itself reports, 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 measures."[332] 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."[333] Japan also amended its basic data protection law, the Act on the Protection of Personal Information, in various ways, and provided additional safeguards through Supplementary Rules to guarantee that data transferred from the European Union enjoyed special protections.[334]

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. Seeking to maintain the EU's adequacy finding, Israel's Ministry of Justice published Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area) on May 7, 2023, establishing four obligations for personal information transferred to Israel from the European Union, Iceland, Liechtenstein, and

---

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").

[329] 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/.

[330] Enhancing Safeguards for United States Signals Intelligence Activities, Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 7, 2022).

[331] *Id.*

[332] European Commission, *European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows* (Jan. 23, 2019), https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421 (emphasis omitted).

[333] *Id.* (emphasis omitted).

[334] 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 (2020).

Norway.[335] The regulations establish a duty to delete upon a written request from the data subject (subject to exceptions), an obligation to limit retention of unnecessary information, an obligation of information accuracy, and an obligation to notify data subjects of the identity of the controller, the purposes of data transfer, and deletion, access, and correction rights of the data subject.[336]

B. Multilateral Response: No Mass-Spying Treaty

States "states enjoy a peacetime right to spy under international law," Asaf Lubin concludes in a recent paper.[337] But that right can be abused, Lubin notes, suggesting limitations on that right.[338] I want to suggest that states should go further, and entrench limits on covert spying by treaty.

Council of Europe Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S.

No. 165

Many will find the prospect of an international treaty to limit spying among the world's biggest powers absurd, bordering on delusional. Yet, it is not as fanciful as it might appear. This is clearly the most ambitious solution to the problem of dangerous data, 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.[339]

An important precedent can be found in the recent Declaration on Government Access to Data held by private sector entities agreed to in 2022 by the Ministers at the Organization for Economic Co-operation and Development (the OECD) meeting on the digital economy.[340] While the OECD does not include China, this agreement among the 38 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. It explicitly commits to restraints "including situations

---

[335] Israeli regulation 5783-2023.

[336] *Id.*

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

[338] *Id.* at 191 (identifying four such 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.").

[339] *See* Andrew Keane Woods, *Litigating Data Sovereignty,* 128 YALE L.J. 328, 393 (2018).

[340] The Organization for Economic Cooperation Development, *Landmark agreement adopted on safeguarding privacy in law enforcement and national security data access* (Dec. 14, 2022), https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm.

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."[341] 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.[342]

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. Reports suggest that the agreement, while imperfect, led to a "dramatic" reduction in cyber-attacks originating in China against U.S. entities.[343]

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 demand that second government prove that it was not responsible, and to take steps against any perpetrators operating within its shores.

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."[344] 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 show that the U.S. intelligence services had hacked into the networks of China's most prestigious university, Tsinghua, which is home to one of six backbone networks in the

[341] The Organization for Economic Cooperation Development, Declaration on Government Access to Personal Data Held by Private Sector Entities, Dec. 13, 2022, OECD Legal 0487.

[342] Council of Europe Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 165, art. 15 (requiring safeguards of proportionality for government authorities exercising powers and procedures for obtaining information); Draft United Nations Convention Against Cybercrime, Aug. 7, 2024, A/AC.291/L.15, art. 24 (same).

[343] 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 ("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." 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, 3:06 am EST, https://www.reuters.com/article/idUSKCN1NE041/.

[344] James Andrew Lewis, *Moving Forward with the Obama-Xi Cybersecurity Agreement*, CSIS, Oct. 21, 2015, https://www.csis.org/analysis/moving-forward-obama-xi-cybersecurity-agreement.

nation.[345] Snowden also claimed that the U.S. National Security Agency had hacked Chinese telecommunications networks, gaining access to millions of text messages.[346]

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." [347] Smith would require that governments "report [cybersecurity] vulnerabilities to vendors rather than stockpile, sell or exploit them."[348] Smith also suggests the creation of an international organization that can investigate and publicly attribute nation-state attacks. The proposal of an anti-digital spying treaty offered here would expand on Smith's suggestion by including prohibitions not just on cyber-attacks, but also on legal orders to compel the disclosure of personal information of foreign persons without sufficient checks and balances.

CONCLUSION

The internet did not come with either national security or 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."[349] "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. 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."[350] 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.[351]

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

---

[345] Lana Lam, *NSA Targeted China's Tsinghua University in Extensive Hacking Attacks, says Snowden*, S. CHINA MORNING POST, June 22, 2013, 11:24pm, www.scmp.com/news/china/article/1266892/exclusive-nsatargeted-chinas-tsinghua-university-extensive-hacking.

[346] Lana Lam & Stephen Chen, *US Spies on Chinese Mobile Companies, Steals SMS data, Edward Snowden*, S. CHINA MORNING POST, 22 June 2013, 9:52 pm, www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companiessteals-sms-data-edward-snowden.

[347] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/; Microsoft, A Cloud for Global Good (2018), https://news.microsoft.com/cloudforgood/policy/microsofts-commitment.html.

[348] *Id.*

[349] David McCabe & Adam Satariano, *The Era of Borderless Data Is Ending*, N.Y. TIMES, May 23, 2022.

[350] Council on Foreign Relations, *Confronting Reality in Cyberspace Foreign Policy for a Fragmented Internet* (2022).

[351] Tim Starks, *Cyber ambassador could soon take on a world of challenges*, WASH. POST, Aug. 2, 2022 at 7:21 a.m. EDT, https://www.washingtonpost.com/politics/2022/08/02/cyber-ambassador-could-soon-take-world-challenges/.

had their medical insurance records hacked.[352] The hackers were able to access the records held by two French service providers for medical insurance companies. 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.[353] They hacked U.S. companies from abroad to access confidential earnings reports and exploit that inside information in the stock market.[354] They were arrested while on vacation in Switzerland and the Maldives.[355] 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. 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.[356]

A decade ago, the U.S. military conceptualized "cyber" as the fifth domain of war, alongside land, sea, air, and space. Over the last 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.

---

[352] Oceane Duboust, *Data of half the population of France stolen in its largest ever cyberattack*, EURONEWS, Feb. 8, 2024, 17:22, updated 20:44, 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.

[353] On August 1, 2024, the U.S. released two Russian hackers in exchange for Evan Gershkovich and other Americans. *See Release of Russian hackers believed to be first U.S. prisoner swap of international cybercriminals*, NBC News, https://www.nbcnews.com/tech/security/us-releases-russian-hackers-evan-gershkovich-prisoner-swap-rcna164746.

[354] *Id.*

[355] *Id.*

[356] 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."). https://www.vectra.ai/blog/the-silent-storm-inside-salt-typhoons-massive-telco-cyberattack ("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," Marc Rogers said. https://www.nextgov.com/cybersecurity/2025/01/gao-mulls-cost-evaluation-nationwide-telecom-hardware-replacement/401963/?oref=ng-homepage-river.