How States Respond to Foreign Surveillance via Social Media: Bans, Breakups, and Beyond

Mapping responses to social media surveillance and manipulation along a spectrum of outright bans, divestiture requirements, comprehensive data privacy laws, and the development of international norms

Rebecca N. Kahn and Jacob M. Fisch*

ABSTRACT

Social media platforms allow States extensive access to user data and influence over public opinion. This article surveys States' legal and policy responses to this reality. It develops a framework for analysis, considering bans, divestiture requirements, comprehensive privacy regulation, and international norm-building.

Using examples from the United States, the European Union, India, Ukraine, and China, the article discusses how responses involve tradeoffs among security, privacy, speech, administrative feasibility, and escalation risks. The article does not present an exhaustive taxonomy or universal solution. Instead, this article presents an organized way to understand how responses operate at different points of intervention and interact across borders. Platform-specific bans or divestiture requirements may address surveillance concerns, but might burden speech, disrupt markets, and invite retaliation. Platform-neutral privacy rules and international norms may offer more durable and evenhanded solutions, despite implementation and enforcement challenges. This survey is intended as a resource for policymakers and researchers.

I. INTRODUCTION

A user attempting to open TikTok in Beijing, New Delhi, Washington, and Brussels will have a vastly different experience in each location. Behind the screen

* Rebecca Kahn received a J.D. in 2025 from New York University School of Law. Jacob "Mendy" Fisch received a J.D. in 2014 from Columbia Law School and an LL.M. in 2025 from Georgetown University Law Center. This article was informed by discussions in seminars with Professors Samuel Rascoff, Pete Pascucci, Lauren Cherry, and Laura Donohue, and incorporates material previously submitted for academic credit. The views expressed are those of the authors and do not represent the views of their respective employers. Although Mr. Fisch is a Navy Judge Advocate, this article does not necessarily represent the views of the Department of Defense or its components, including the Department of the Navy. © 2026, Rebecca N. Kahn & Jacob M. Fisch.

are divergent regulatory choices that reflect, among other things, how States balance concerns about foreign surveillance, information control, economic leverage, and data governance. This article surveys these regulatory choices, including China's firewall, bans in India and Ukraine, U.S.-style divestiture and investment review, and the European Union's ("EU") comprehensive data protection framework. We present these cases as instances of three types of tools (bans, breakups, and broad regulations) that States utilize to manage the risks of surveillance and manipulation over social media. We also present a fourth category, which we suggest deserves more prominence: development of international rules and guidelines.

A. TikTok as the Motivating Case Study

The long road toward TikTok regulation in the United States motivated this article and serves as a central case study. The difficult tradeoffs made during the fitful, five-year journey underscore the complexity of the social media regulatory puzzle. The effort began in 2020, when the Committee on Foreign Investment in the United States ("CFIUS") determined that the Chinese government's access to data harvested from the social media app's U.S. user base was a national security risk.[1] When the CFIUS process stalled, Congress passed the 2024 Protecting Americans from Foreign Adversary Controlled Applications Act ("PAFACAA"), requiring U.S. companies to stop offering access to TikTok unless ByteDance, TikTok's China-based owner, divested by January 19, 2025.[2]

The U.S. Supreme Court's willingness in *TikTok Inc. v. Garland* to accept these sweeping regulatory measures despite First Amendment challenges reflected the three branches' remarkable consensus that the status quo—allowing China continued access to TikTok's U.S. user base—constituted an unacceptable national security threat.[3] Yet, implementation of the court-sanctioned law was repeatedly delayed in order to find a buyer for TikTok that was not "controlled by a foreign adversary."[4]

1. *See* Petition for Review at 45–49, TikTok Inc. v. Committee on Foreign Inv., No. 20-1444 (D.D.C. Nov. 10, 2020) (CFIUS letter outlining national security risks of TikTok) [hereinafter Petition for Review].

2. Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, 138 Stat. 955 (2024) (codified as a statutory note under 15 U.S.C. § 9901). The deadline of January 19, 2025, was determined by adding 270 days to the date of PAFACAA's enactment. *Id.* § 2(a)(2)(A).

3. TikTok Inc. v. Garland, 604 U.S. 56, 73–74 (2025) (per curiam) (applying intermediate scrutiny, the Court agreed that preventing China from capturing personal data of U.S. users is an "important government interest.").

4. 15 U.S.C. § 9901 note § 2(g)(3)(A). In September 2025, President Donald Trump delayed enforcement of PAFACAA until January 23, 2026. Saving TikTok While Protecting National Security, Exec. Order No. 14,352, 90 Fed. Reg. 47,219 (Sep. 25, 2025) [hereinafter EO 14352]. This was the latest in a series of delays. *See, e.g.*, Further Extending the TikTok Enforcement Delay, Exec. Order No. 14,310, 90 Fed. Reg. 26,913 (June 19, 2025); Sapna Maheshwari, *Trump to Again Extend TikTok's Reprieve from U.S. Ban*, N.Y. TIMES (June 17, 2025), https://perma.cc/NFQ2-X8JJ.

Negotiations continued through 2025.[5] Finally, in December 2025, ByteDance agreed to spin off a new corporate entity (in which it retained a minority stake) to control U.S. user data.[6] When the deal took effect in January 2026, TikTok remained operational in the United States, with U.S. user data presumably more secure.[7] However, questions lingered about the deal's efficacy,[8] highlighting the challenge of how best to counter foreign State surveillance in the absence of an international legal framework or clear international norms.

B. Method and Limitations

This article compares four categories of State responses to the dual risks of foreign State surveillance and foreign influence or manipulation conducted through social media platforms: outright bans, divestiture requirements, data privacy laws, and development of international rules and guidelines. Section II describes State access to social media data. Section III presents case studies. We consider India's ban of TikTok, Ukraine's ban of VK Group, and China's "Great Firewall" as examples of bans motivated in part by concerns about surveillance and foreign influence. We examine PAFACAA and CFIUS-driven divestitures as examples of divestiture requirements. The article next discusses the EU's General Data Protection Regulation ("GDPR") as an example of a comprehensive data privacy law that has been enforced against specific platforms, including Facebook (Meta)

---

5. On September 25, 2025, President Trump announced a proposed "framework agreement" for ByteDance to divest from TikTok. *Fact Sheet: President Donald J. Trump Saves TikTok While Protecting National Security*, WHITE HOUSE (Sep. 25, 2025), https://perma.cc/9CGJ-CBRX [hereinafter *TikTok Framework Fact Sheet*]. On October 30, 2025, Treasury Secretary Scott Bessent announced that an agreement was "finalized." Julia Shapero, *Bessent Says TikTok Deal Finalized*, THE HILL (Oct. 30, 2025), https://perma.cc/XRK5-J9V7.

6. David Shepardson, *China's ByteDance Signs Deal to Form Joint Venture in Step to Avoid US TikTok Ban*, REUTERS (Dec. 19, 2025), https://perma.cc/Z7DL-K4KC; Sara Fischer, *Scoop: TikTok Signs Deal for U.S. Unit After Yearslong Saga*, AXIOS (Dec. 18, 2025), https://perma.cc/EVB8-5Z3S.

7. ByteDance will own 19.9% of the new entity, called TikTok USDS Joint Venture LLC. The rest will be owned by a "consortium of investors," including the U.S.-based Oracle and Silver Lake, as well as MGX, a fund controlled by Abu Dhabi. *Announcement from the New TikTok USDS Joint Venture LLC*, TIKTOK (Jan. 22, 2026), https://perma.cc/WH3L-T3A6 [hereinafter *TikTok USDS Announcement*]; Zach Everson, *Abu Dhabi Fund MGX Emerges as Key Player in Two Major Trump-Era Deals*, FORBES (Oct. 15, 2025), https://perma.cc/WM3R-HWRX. The deal is further discussed in § III.B.1 *infra*.

8. Questions focused on the lack of transparency surrounding the deal, ByteDance's continued ownership of the recommendation algorithm, and the ongoing relationship between the new entity and ByteDance. *See*, *e.g.*, *National Security Experts Argue U.S. TikTok Deal Falls Short*, PBS (Jan. 23, 2026), https://perma.cc/627D-PZ5S; Adam Conner, *The TikTok Deal Leaves Many Questions Unanswered*, CTR. FOR AM. PROGRESS (Jan. 22, 2026), https://perma.cc/KV3W-GZ28; John Moolenaar, *Moolenaar: Questions Need To Be Answered on TikTok Deal*, H. SELECT COMM. ON STRATEGIC COMPETITION BETWEEN THE U.S. & THE CHINESE COMMUNIST PARTY (Jan. 23, 2026), https://perma.cc/V5RB-VA2C ("The Chinese Communist Party cannot be allowed to weaponize an app to divide and weaken our country. Does this deal ensure China does not have influence over the algorithm? Can the parties involved assure Americans their data is secure? Those are questions that need to be answered as the Select Committee does oversight of this deal."). These questions are further discussed in § III.B.3 *infra*.

and TikTok.[9] In Section IV, we present the development of international rules and guidelines as a complement to regulation and a solution to the coordination problem created by State behavior. We propose two promising areas for further development: the rule against intervention and the Organisation for Economic Co-operation and Development ("OECD") Privacy Guidelines.

This article does not offer a comprehensive taxonomy of every global surveillance regulation; rather, the categories represent some of the most common high-level structural interventions that States have used in response to surveillance risk.[10] The article does not definitively recommend one strategy over another. The article also does not comprehensively interrogate or examine States' regulatory objectives. Although governments frequently justify measures regulating social media in national security terms, the article recognizes that States use them to pursue overlapping objectives, which may include controlling domestic speech or monitoring their own populations.[11]

C. Contributions to the Literature

Treating State responses as a typology is not merely an exercise in classification. This article is novel in identifying distinct regulatory levers: platform access (a ban, i.e., whether the platform can operate at all), platform ownership (divestiture, i.e., who can operate the platform), data flows (comprehensive data privacy regulation, i.e., what data can be collected/transferred under what conditions), and State conduct (international norms, i.e., how States interact with each other).

---

9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR], https://perma.cc/748N-PMEH. We also briefly discuss the EU's Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 Oct. 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1 [hereinafter DSA].

10. As stated, these categories do not exhaust the universe of State responses. One set of restrictions to discuss in future research are those specifically targeting data transfer, such as security reviews for cross-border transfers or prohibitions on data brokers selling to certain countries. These are explored briefly in the context of the GDPR in Section III.C.1 and III.C.2; for a narrower effort in the United States, see Protecting Americans' Data from Foreign Adversaries Act of 2024, 15 U.S.C. § 9901 (restricting data brokers from selling information about individuals residing in the United States to "foreign adversaries"). Another response mode not explored is gathering information about the vulnerability of social media companies using mandatory audits. *See*, *e.g.*, DSA, *supra* note 9, art. 37. Sector-scoped restrictions such as bans of TikTok on government devices are discussed briefly *infra* note 85, but bear further discussion. Finally, Section IV *infra* discusses several areas of international law but does not focus on binding agreements; this could be another area for development.

11. In 2024, Freedom House observed that "Chinese internet users have faced the world's worst conditions for internet freedom for a decade," noting that the Communist Party "continues to tighten control over all aspects of life and governance, including the state bureaucracy, the media, online speech, religious practice, universities, businesses, and civil society associations." *Freedom on the Net 2024: China*, FREEDOM HOUSE (Oct. 2024), https://perma.cc/226V-2EPB. The inclusion of a country's strategy in our taxonomy does not imply that the country's goals or policies are equivalent to those of the other countries. China's policy stands out in that it is part of an extensive landscape of censorship. This article does not comment normatively (i.e., determine whether the strategies discussed are moral or ethical).

In the short time that State-sponsored social media operations have been possible, State response options have not been surveyed in this way. This survey aims to be a resource for policymakers and researchers in this emerging field.

Categorizing response options allows us to draw comparative lessons from each strategy. The mapping highlights how each regulatory lever comes with tradeoffs, affecting values such as individual privacy, freedom of speech, and free and fair markets. The mapping also allows us to observe more clearly how threats over social media fuel unilateral regulatory actions and how these actions can then inspire reciprocal measures. Building on these lessons, this article observes that while each State has its own unique set of considerations (e.g., civil-liberties costs, escalation tolerance, platform substitution options), an effective long-term strategy is likely to involve the adoption of comprehensive data privacy laws and the development of international rules and norms. When implemented well, these approaches bring the advantages of fairness and equal enforcement that are missing in the first two approaches.

D. Game Theory Terminology as a Lens and Future Research Direction

States' adoption of surveillance-related rules occurs in an interactive environment that has long been analyzed using game-theoretic tools.[12] This article incorporates concepts from international relations game theory to better explain our observations about States' choices. Additionally, by categorizing regulatory responses and discussing the patterns of interdependency among them, this article helps set the stage for future work applying game theory to social media regulation.

Game theory concepts that are useful for understanding some of the actions and reactions discussed in this article include "offensive" and "defensive" moves;[13] the "security dilemma;"[14] assurance games and coordination failures;[15]

12. *See, e.g.*, Robert Axelrod & Robert O. Keohane, *Achieving Cooperation under Anarchy: Strategies and Institutions*, 38 WORLD POL. 226, 226–54 (Oct. 1985) (analyzing cooperation/discord in world politics through factors like the "shadow of the future," number of players, reciprocity, and issue-linkage via "multilevel games," and describing how actors try to change contexts through institutions and norms); BEN BUCHANAN, THE CYBERSECURITY DILEMMA: HACKING, TRUST AND FEAR BETWEEN NATIONS (2017) (a recent application of game-theoretic concepts to State interactions in cyberspace in particular).

13. "Defensive" actions attempt to maintain the status quo, while offensive actions seek to accrue some new benefit to the actor. Professor George Quester explains: "In sports, everyone wants to win, but there are times when the best one can do is to keep the score as it is (e.g., when the other team is at bat in baseball; when the other team has the ball in football). . . . At other times, the environment may suggest great advantages for launching an attack." George H. Quester, *Offense and Defense in the International System*, *in* OFFENSE, DEFENSE, AND WAR 51, 51 (Michael Brown, et al., eds., 2004). The framing of actions as "offensive" or "defensive" is helpful to understand each approach discussed in this article.

14. The security dilemma concept explains why even measures that sound defensive—banning a foreign app, for example—can be interpreted by rivals as offensive. This then might prompt rivals to match or escalate. This is a dynamic that drives arms races. Shiping Tang, *The Security Dilemma: A Conceptual Analysis*, 18 SEC. STUD. 587, 588–89, 591–93 (2009).

15. Assurance games and coordination failures are concepts that can help explain why coordination can stall: for example, even if every country might benefit from a common standard (for example, GDPR-level privacy conduct), few countries are willing to go first and sacrifice economic gains or intelligence access if other countries might defect. A "stag-hunt" or assurance game is a variant of the

reciprocity;[16] and multilevel games.[17] States' strategies are often interdependent,[18] and States have difficulty making credible commitments.[19] Although a detailed discussion is left for future work, these concepts help frame the article's claim that States' moves (ban, divestiture, or domestic privacy statutes) reverberate abroad and back at home. These game theory principles make sense of seemingly sui generis decisions. They also clarify why the proposed fourth path, developing shared norms, is a logical strategy for escaping the surveillance spiral. Shared norms enable States to shift toward a coordination equilibrium with clearer commitments, monitoring, and reciprocity.

---

prisoner's dilemma where cooperation brings the biggest payoff for both players, but defection yields the defector the second-best payoff. As described by Uri Weiss and Joseph Agassi:

> This is illustrated by two hunters who choose simultaneously whether to hunt a stag or rabbits. They succeed only if they both go for a stag, and each player achieves the best result—the stag. A player who goes for a stag alone is met with absolute failure. A player who goes for a rabbit alone wins all the rabbits, which is the second-best result, while both going for the rabbits mutually gives every player half of the rabbits—the third best result.

Uri Weiss & Joseph Agassi, *Game Theory for International Accords*, 16 S.C. J. INT'L L. AND BUS., no. 3, 2020, at 1, 5–6 (2020).

16. Surveillance controversies are not one-off. Platforms and laws evolve quickly and repeatedly. When states engage in repeated interactions that invite an escalation of reciprocal offensive actions, this is known as retaliation, and authors use the term "retaliation dynamics" to describe how moves invite countermeasures. *See*, *e.g.*, Brandon Valeriano & Benjamin Jensen, *The Myth of the Cyber Offense: The Case for Restraint*, CATO INST. (Jan. 15, 2019), https://perma.cc/F7LH-MVGH (Table 1 compares cyber incident severity with response severity to analyze "retaliation dynamics" following cyber incidents). On the other hand, reciprocity can also involve cooperation. Iterative and reciprocal interaction makes reputation important. Instruments such as the EU's adequacy review under the GDPR help sustain restraint. Successful norm-building requires credible signals that other countries will reciprocate. Institutional devices, like data-adequacy rulings and mutual agreements, can help lock in coordination. For a discussion of this during the Covid pandemic, see JENNIFER M. WELSH, INTERNATIONAL COOPERATION DURING THE COVID-19 PANDEMIC: LEARNING FROM PAST EFFORTS TO ADDRESS COMMON THREATS (2022).

17. The concept of "multilevel" games helps explain the tension that occurs when a country must consider multiple goals for which to optimize. For example, when intelligence agencies value data access, but legislatures value privacy and economic openness, bargains can unravel domestically, as seen in the United States' struggle to implement PAFACAA or federal privacy bills. For an application of the concept of "two-level" games to illustrate the decisions of States on the international stage, satisfying both national-level and international-level priorities, see Robert Putnam, *Diplomacy and Domestic Politics, The Logic of Two-Level Games*, 42 INT'L ORG. 427, 434 (1988). For an analysis of the Cuban Missile Crisis as a "multilevel" game, see FRANK C. ZAGARE, GAME THEORY, DIPLOMATIC HISTORY AND SECURITY STUDIES 67–72 (2019).

18. "[G]ames all share the common feature of interdependence. That is, the outcome for each participant depends on the choices (strategies) of all." Avinash Dixit & Barry Nalebuff, *Game Theory*, ECONLIB (Feb. 5, 2018), https://perma.cc/5QGW-44PN. In the examples presented, one State's regulatory actions change other States' incentives and strategies ("strategic interdependence"). For example, the EU's choice to regulate via the GDPR led the U.S. to provide a redress mechanism for EU members and others, as discussed *infra* Section III.C.2.

19. "At the heart of the problem of credible commitment is the strategic interdependence of two or more actors making sequenced choices." *Credible Commitment*, *in* INTERNATIONAL ENCYCLOPEDIA OF POLITICAL SCIENCE 487, 487 (Bertrand Badie, Dirk Berg-Schlosser & Leonardo Morlino eds., 2011). A "credible commitment" problem arises when one State seeks to convince another State that it will follow a particular course of action in a particular circumstance. A State may constrain its options "to induce beneficial actions from other players." *Id.* "'[B]urning one's bridges' may elicit more advantageous behavior from one's soldiers (or one's opponents)." *Id.*

II. STATE ACCESS TO SOCIAL MEDIA DATA

The policies discussed in this paper are primarily animated by efforts to curb surveillance operations conducted by three State actors: the United States, China, and Russia. These actors have both a cybersecurity interest in protecting their own citizens and networks and a strategic espionage interest in exploiting foreign data flows for domestic intelligence purposes.[20] These States' intelligence communities and domestic laws enable a high level of access to information from domestic social media companies.[21] Their access to these platforms goes beyond what can be purchased or scraped.[22] In some cases, the access may enable manipulation of the user base as States combine their knowledge of users with the ability to control content on the platform. This section discusses a few of these three States' domestic social media platforms and the laws allowing these States access to platform data.

---

20. Important to note is that the United States, China, and Russia operate under markedly different constitutional and political constraints on freedom of expression and access to information, and the role of censorship and regime control over information governance is substantially more salient in the Chinese and Russian contexts. Those differences matter for both the baseline level of State control over digital spaces and the kinds of justifications that are politically available to them for surveillance regulations. Nonetheless, each State confronts the same dilemma: how to secure domestic information from foreign exploitation while keeping their own surveillance options open and preserving participation in the global internet. Therefore, we analyze policy responses using a common analytic framework. This permits a more comparative account of how common incentive structures shape regulatory choices, as discussed above.

21. The scope and enforceability of citizen protections in these countries differ substantially. In particular, the United States' constitutional and statutory frameworks recognize a right to privacy in some situations and provide for an independent judiciary that provides ex ante and ex post constraints on executive action related to information gathering. These institutional checks and regulations are significantly weaker in China and Russia. That said, U.S. law still authorizes extensive government access to data held by U.S. companies regarding non-USPs.

22. In this discussion of State surveillance and manipulation via State-owned or domestic social media companies, it is important to note that States retrieve much information of intelligence value from corners of the internet that they do not control. States may do this by purchasing large datasets of commercially available information and by scraping publicly available information. *See*, *e.g.*, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, Exec. Order No. 14,117, 89 Fed. Reg. 15,421 (Feb. 28, 2024) [hereinafter EO 14117] ("Access to Americans' bulk sensitive personal data . . . by countries of concern through data brokerages [or] third-party vendor agreements . . . poses particular and unacceptable risks to our national security."); *Justice Department Issues Final Rule Addressing Threat Posed by Foreign Adversaries' Access to Americans' Sensitive Personal Data*, U.S. DEP'T OF JUST. (Dec. 27, 2024), https://perma.cc/9S9Q-A9WZ (discussing efforts of countries of concern to purchase Americans' bulk personal data and how the Justice Department's rule implementing EO 14117 prevents that). As an example of open-source information, Ukrainians have used Russian social media posts to which they have access to determine unit positions. *See*, *e.g.*, Jack Hewson, *Ukrainian Company Uses Social Media, Open Source Technology to Counter Russian Invasion*, PBS NEWS (Apr. 19, 2023), https://perma.cc/G9EJ-YNYF. Finally, sophisticated actors can and do steal personal information from other countries' companies. *See* Sarah Krouse, Dustin Volz, Aruna Viswanatha & Robert McMillan, *U.S. Wiretap System Targeted in China-Linked Hack*, WALL ST. J. (Oct. 5, 2024), https://perma.cc/N43W-RM96. While some of the responses to foreign surveillance methods overlap with those discussed in this footnote, this article primarily focuses on the extraordinary access that some States enjoy to the data accumulated by companies that are subject to their surveillance laws.

A. U.S. Access to American Social Media Company Data

Title VII of the Foreign Intelligence Surveillance Act ("FISA") allows U.S. intelligence agencies to compel U.S. service providers to hand over information about any individual or entity located overseas that is not a U.S. Person ("USP").[23] This authority was added in 2008; unlike other parts of FISA, it does not require individualized judicial review of surveillance targets.[24] Instead, the Attorney General ("AG") and Director of National Intelligence ("DNI") provide annual certifications to the Foreign Intelligence Surveillance Court ("FISC") regarding each intelligence agency's program.[25] Once an agency's program is approved by the FISC, the agency (pursuant to the authority of the AG and DNI) can issue directives to U.S. companies requiring them to provide data responsive to certain selectors (sometimes called "targeting directives"), as long as the directives are intended to retrieve foreign intelligence information about non-USPs located outside the United States.[26] A company receiving a directive can challenge the directive at the FISC, but there is no way for someone whose data is being collected to challenge a directive.[27]

Agencies using this authority must develop and adhere to rules for targeting (requesting data from U.S. companies), querying (looking up information in data that has already been received), and minimization of stored data (to mitigate the risk of their activities to USPs' privacy).[28] While annually approved procedures are initially classified, the Office of the Director of National Intelligence ("ODNI") has declassified some past-year procedures, shedding additional light on these methods.[29] Under FISC-approved targeting procedures, tasking has to be

---

23. 50 U.S.C. § 1881a(a) ("[T]he Attorney General and Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."). USPs outside the United States cannot be targeted. *Id.* § 1881a(b)(3). USPs are defined as citizens or legal permanent residents of the United States, U.S. corporations, and organizations that have a substantial number of USPs. *Id.* § 1801(i).

24. Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L. & PUB. POL'Y 117, 154, 158 (2015).

25. 50 U.S.C. § 1881a(g), (h), (j).

26. *Id.* § 1881a(i)(1)(A). Service providers may challenge these directives in the Foreign Intelligence Surveillance Court. *Id.* § 1881a(i)(4). The statute does not set any requirements that a target be suspected of illegal acts as long as the target is reasonably believed to be located outside the United States, a significant purpose of the targeting is to acquire foreign intelligence, and the acquisition is otherwise consistent with the Constitution. *Id.* § 1881a(d)(1)(A), (h)(2)(A)(v).

27. *Id.* § 1881a(i)(4).

28. *Id.* § 1881a(j)(2).

29. *See, e.g.*, FED. BUREAU OF INVESTIGATION, PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 (2023), https://perma.cc/9RYZ-DUNK; CENTRAL INTELLIGENCE AGENCY, MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH THE ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2020), https://perma.cc/52ZL-TFN5; NAT'L SEC. AGENCY, QUERYING PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN

reasonably designed to acquire foreign intelligence information from non-USPs "reasonably believed to be located outside the United States."[30] Intentional targeting of USPs or anyone in the United States, targeting a non-USP outside the United States with the intent to receive information about someone in the United States ("reverse targeting"), or intentional acquisition of domestic-only communications is forbidden.[31] FISC-approved procedures add detail to the requirements. For example, the National Security Agency's ("NSA") 2023 targeting procedures required documentation of why NSA determined that the target was a non-USP located outside the United States (the "foreignness determination"), included oversight procedures, and required post-targeting analysis.[32]

Querying procedures govern access to unminimized repositories. For example, the Federal Bureau of Investigation's ("FBI") approved procedures from 2024 require all personnel querying data repositories to be trained; those personnel may only query a repository for the purpose of retrieving foreign intelligence information.[33] The procedures require personnel to provide a written, specific factual basis for why a query is reasonably likely to retrieve foreign intelligence information and to maintain auditable logs with justifications.[34] Agencies must record any query term associated with USPs.[35] The FBI, which investigates domestic crimes in addition to its counter-espionage mission, may not use a query term solely to extract evidence of crimes unless necessary to address imminent threats to life or serious bodily harm.[36]

Minimization Procedures limit retention and dissemination of incidentally acquired USP information.[37] For example, the NSA's 2023 procedures mandate prompt destruction upon recognition of domestic-only items or other communications not to or from the tasked selector, and require destruction of raw data after five years from the expiration of the certification authorizing the collection.[38] The NSA's procedures provide that if the Department of Justice's ("DOJ") National

---

INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2020), https://perma.cc/TR2K-8RQ2.

30. 50 U.S.C. § 1881a(d)(1)(A).

31. *Id.* § 1881a(b).

32. NAT'L SEC. AGENCY, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 1, 9–12 (2022), https://perma.cc/2338-HGA4 (the procedures are dated March 2022, but were submitted for approval in 2023).

33. FED. BUREAU OF INVESTIGATION, QUERYING PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 1, 4 (2024), https://perma.cc/CM6Y-YN76.

34. *Id.* at 4, 6–7.

35. 50 U.S.C. § 1881a(f)(1)(B).

36. *Id.* § 1881a(f)(2).

37. *Id.* §§ 1881a(e), 1801(h).

38. NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 6 (2023), https://perma.cc/TL7P-MKDE [hereinafter 2023 NSA MINIMIZATION PROCEDURES].

Security Division determines that certain selectors were improper, the NSA must sequester and purge the material (e.g., place it on a Master Purge List) and recall any disseminations; the NSA must notify the FISC if it is not able to do this.[39]

Requesting information via a targeting directive often results in an agency receiving information it was not looking for; agencies store this information and query it for other foreign intelligence purposes.[40] As discussed, if information is collected as the result of selectors (search terms) that were not consistent with the targeting directive or violated targeting procedures, agencies are required to purge or destroy this information under their FISC-approved minimization procedures.[41] However, if information about individuals who were not targeted is incidentally collected pursuant to valid selectors (for example, a foreign target communicated with a USP), none of the above-discussed laws or procedures require deletion of this information. The information can be kept and used, provided the minimization and querying rules are followed, including restrictions for USP query terms.[42]

The extent of the surveillance enabled by FISA came into focus for the rest of the world when, in 2013, Edward Snowden revealed programs that were enabled by Title VII.[43] One program in particular, the NSA's PRISM program, exemplified the breadth of information that U.S. agencies compelled from service providers without an individualized warrant.[44] The Snowden leaks also shed light on the practice of "upstream" collection, through which data merely passing through the United States can be intercepted.[45] The revelations resulted in litigation against American companies in the European Union ("EU"). For example, when Austrian Max Schrems found out that his information held by Facebook was

39. *Id*. at 9.

40. *See* Donohue, *supra* note 24, at 188, 237–39.

41. 50 U.S.C. §§ 1881a(e), 1801(h); *see also* 2023 NSA MINIMIZATION PROCEDURES, *supra* note 38, at 6, 9.

42. 50 U.S.C. § 1881a(e)(1), (f)(1).

43. Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST (June 12, 2023), https://perma.cc/FYJ8-MEEX; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), https://perma.cc/EC35-TZSX. A different part of FISA, Section 215 of the USA PATRIOT Act (at the time codified as Title V of FISA) was the legal basis for another program that collected Americans' phone records. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), https://perma.cc/SV9W-WC5F; Kenton Powell, *The Legal Case*, GUARDIAN (Nov. 1, 2013), https://perma.cc/L7LH-FDP6.

44. The NSA documents released by Snowden showed the NSA received details from American tech companies including email, chat, video conferencing, logins, social network activity, and more. *NSA Prism Program Slides*, GUARDIAN (Nov. 1, 2013), https://perma.cc/MP2E-A7FX; *see also* T.C. Sottek & Janus Kopfstein, *Everything You Need to Know About PRISM*, VERGE (July 17, 2013), https://perma.cc/TG9W-QXJF.

45. *See* Sottek & Kopfstein, *supra* note 44. The NSA later announced that it would narrow the type of "upstream" internet information that it collected to just information to or from the target. *NSA Stops Certain 702 "Upstream" Activities*, NAT'L SEC. AGENCY (Apr. 28, 2017), https://perma.cc/BA48-277F.

possibly swept up in PRISM, he sued and won.[46] The revelations also spurred the passage of the EU's General Data Protection Regulation ("GDPR").[47]

Twelve years after the Snowden leaks, many of the same authorities remain in place, although the realities on the ground are different. Encryption has made it harder for agencies to read many private messages and internet traffic, even if they are intercepted or provided.[48] Agencies have targeting procedures that, if followed, would result in narrower collection programs than the version of PRISM revealed by Snowden.[49] As a result of multiple rounds of *Schrems* litigation, the United States recognized limited privacy rights of some non-Americans.[50] Still, U.S. law and policy are focused on the privacy rights of people within the United States and USPs abroad. Non-USPs outside the United States are not protected by the Fourth Amendment.[51] FISA does not require a warrant to obtain non-USP data from U.S. providers, and the Executive Order ("EO") that provides presidential authority to the intelligence community, EO 12333, only mandates protections for USPs.[52] U.S. intelligence agencies can, without a warrant, gather

46. Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650 (Oct. 6, 2015). The Court of Justice of the European Union relied in part on the existence of the PRISM program to find that a previous data security agreement between the United States and the European Union provided inadequate safeguards for EU citizens and the system inadequately protected "fundamental rights," including the "right to respect for private life and the right to protection of personal data." *Id.* ¶¶ 1, 21, 81, 98. For discussion of subsequent litigation by Schrems, see *infra* Section III.C.

47. *See* Hallie Coyne, *The Untold Story of Edward Snowden's Impact on the GDPR*, CYBER DEF. REV., Fall 2019, at 65, 67, 69–70; Samuel Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 666 (2016) ("The revelations had the effect of recalibrating the relative power of privacy-minded European politicians, who had been successfully sidelined by more security-minded officials for a decade.").

48. *See* Alexis Hancock, *We Encrypted the Web: 2021 Year in Review*, ELEC. FRONTIER FOUND. (Dec. 27, 2021), https://perma.cc/RXX4-HVTE.

49. PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 65–69 (2023) [hereinafter PCLOB]. Also, the version of Title V of FISA in effect during the Snowden leaks (known as Section 215), enabling expansive collection of business records, lapsed on March 15, 2020, and Title V reverted to a more restrictive provision. *Id.* at 31. *See also* OFF. OF THE DIR. FOR NAT'L INTEL., HOW FISA SECTION 702'S COMPLIANCE & OVERSIGHT HAVE GROWN TO STRENGTHEN PRIVACY AND CIVIL LIBERTIES PROTECTIONS FOR U.S. PERSONS (2023), https://perma.cc/M5LL-G2JG.

50. Exec. Order No. 14,086, 87 Fed. Reg. 62,283 (Oct. 7, 2022) [hereinafter EO 14086]. The EO requires agencies to consider the privacy rights of non-USPs in decisions about data collection and establishes a way for some foreigners (including EU citizens) to file complaints about how their data is stored. *Id.* §§ 2(c)(iii)(A)(1), 3(d).

51. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . ."); United States v. Verdugo-Urquidez, 494 U.S. 259, 261, 265–67 (1990) (determining that a "nonresident alien" living abroad was not contemplated by the Fourth Amendment). "The people" protected by the Fourth Amendment "refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community." *Id.* at 265. While *Verdugo-Urquidez* did not define "the people" in the same terms as the FISA definition of USPs presented in note 23 *supra*, the definition of non-USPs abroad (as defined by FISA) aligns with the definition of "nonresident alien" in *Verdugo-Urquidez*; those individuals or entities have not "developed sufficient connection" to the United States to be considered part of "the people."

52. 50 U.S.C. § 1881a; United States Intelligence Activities, Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4,075 (Jan. 23, 2003), Exec.

extensive information about non-USPs outside the United States who use U.S. social media platforms; they are increasingly relying on this authority.[53]

B. China's Access to Chinese Social Media Company Data

In *TikTok Inc. v. Garland*, the Supreme Court pointed to Chinese laws requiring Chinese companies to "assist or cooperate" and "surrender data" to the Chinese government to suggest that ByteDance, TikTok's parent company, would provide Americans' data to China; the Court found that preventing such access to U.S. user data was an important government interest.[54] Similarly, in its investigation of TikTok, CFIUS identified China's laws as a reason to require ByteDance to divest from the company.[55] CFIUS cited the existence of Chinese Communist Party ("CCP") members installed in ByteDance's Chinese subsidiary as evidence of China's control over both data received and content provided on ByteDance apps.[56]

Three Chinese laws—the National Security Law, the National Intelligence Law, and the Cybersecurity Law—form the backbone of the legal framework supporting China's surveillance. These laws are broad and lack the checks and court approval requirements of FISA. The National Security Law requires "citizens and organizations" to "provide[] public security organs, state security organs or relevant military organs with necessary support and assistance" and provide the "conditions to facilitate" this assistance.[57] Enterprises must "cooperate with relevant departments in employing relevant security measures."[58] The National Intelligence Law authorizes "intelligence work institutions" to request organizations provide "necessary support, assistance, and cooperation."[59] It permits

---

Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), and Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (July 30, 2008) [hereinafter EO 12333]. § 2.3 of EO 12333 limits the intelligence community's ability to collect, retain, or disseminate information about USPs. *See also id.* § 1.1(b).

53. *See* PCLOB, *supra* note 49, at 3 ("During calendar year 2022, approximately 246,073 non-USPs located abroad were targeted under Section 702. The number of Section 702 targets has nearly doubled over the last five years.").

54. *Id.* at 73 (since the justices determined that PAFACAA was content-neutral, the existence of this important governmental interest allowed the law to withstand intermediate scrutiny).

55. Petition for Review, *supra* note 1, at 45–46 (Assistant Secretary of Investment Security Thomas Feddo's letter to ByteDance's attorneys).

56. *Id.* at 45 (In the meetings, ByteDance officials discuss "'doing a proper job of spreading positive energy,' reportedly a propaganda euphemism.").

57. Zhonghua Renmin Gongheguo Guojia Anquan Fa (中华人民共和国国家安全法) [National Security Law of the People's Republic of China], Order of the President No. 29/2015 (promulgated by the Standing Comm. Nat'l People's Cong., July 1, 2015, effective July 1, 2015), art. 77, 2015:4 GAZETTE OF THE STANDING COMMITTEE OF THE NATIONAL PEOPLES' CONGRESS 701, 705, *translated in National Security Law*, CHINA L. TRANSLATE (July 1, 2015), https://perma.cc/6FP3-N97W [hereinafter National Security Law].

58. *Id.* art. 78.

59. Zhonghua Renmin Gongheguo Guojia Qingbao Fa (中华人民共和国国家情报法) [National Intelligence Law of the People's Republic of China], Order of the President No. 69/2017 (promulgated by the Standing Comm. Nat'l People's Cong., June 27, 2017, effective June 27, 2017, amended Apr. 27, 2018), art. 14, 2017:4 GAZETTE OF THE STANDING COMMITTEE OF THE NATIONAL PEOPLES' CONGRESS 474, 475, *translated in PRC National Intelligence Law (as Amended in 2018)*, CHINA L. TRANSLATE (June 27, 2017), https://perma.cc/B2NP-BB9W [hereinafter National Intelligence Law].

intelligence officers to "read or collect relevant files" and enter "restricted areas."[60] It mandates that organizations comply with these requests and "support, assist, and cooperate" with intelligence efforts.[61] While the National Intelligence Law caveats that intelligence efforts must "respect and protect human rights, and shall preserve the lawful rights and interests of individuals and organizations," there is no mechanism within the law to accomplish this—i.e., there is no external, judicial, or parliamentary mechanism within the law comparable to FISA's court-based model.[62] The Cybersecurity Law strengthens the system created by the other two laws by requiring service providers to store "personal information or important data during operations" within China.[63] That law reiterates that network operators must support national security agencies by providing technical support and assistance.[64]

China's legal framework, the Communist Party's presence within social media companies, and reports of surveillance led U.S. national security experts to warn that the Chinese government gathers intelligence and manipulates content on TikTok and other Chinese-owned apps.[65] The risk extends to Chinese-based apps such as WeChat, and beyond data gathering to promotion of pro-China views.[66]

---

60. *Id.* art. 16.

61. *Id.* art. 7.

62. *Id.* art. 8.

63. Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China], Presidential Order No. 53/2016, (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 37, 2016 XINHUA SHE 1, 2, *translated in* Rogier Creemers, Graham Webster & Paul Triolo, *Cybersecurity Law of the People's Republic of China*, DIGICHINA (June 29, 2018), https://perma.cc/SB9E-YBB4 [hereinafter Cybersecurity Law]. The law provides that if "business requirements" require storage outside the mainland, Chinese agencies must be consulted for a security assessment. *Id.* TikTok executives insist that all U.S. TikTok data is kept in the United States, but many U.S. lawmakers doubted that assertion. *See* Matt Perault, *What Happened to TikTok's Project Texas?*, LAWFARE (Mar. 20, 2024), https://perma.cc/V4AW-DL8V.

64. Cybersecurity Law, *supra* note 63, at art. 28.

65. The Joint Appendix in *TikTok Inc. v. Garland* contains a statement from Casey Blackburn, Assistant Director of National Intelligence at the Office of Economic Security and Emerging Technologies. *See* Joint Appendix at 625–54, TikTok Inc. v. Garland, 604 U.S. 56 (2025) [hereinafter TikTok Joint Appendix]. Mr. Blackburn warned that TikTok "could be used by the PRC against the United States in two principal ways: malign foreign influence targeting U.S. persons, and collection of sensitive data of U.S. persons." *Id.* at 628. Explaining that China has built datasets of U.S. citizens for years, including financial and health information, Mr. Blackburn cited statements of former TikTok employees about data being sent to China. *See id.* at 634–35, 653. Much of Mr. Blackburn's sources are redacted from the report, however. *See id.* at 625–54. *See also* Petition for Review, *supra* note 1, at 45–49 (including CFIUS review letter outlining national security risks of TikTok).

66. *See, e.g.*, Joel Finkelstein, Lee Jussim, John Farmer, Alex Goldenberg, Jacob Zucker, Danit Finkelstein & Sonia Yanovsky, *The CCP's Digital Charm Offensive: How TikTok's Search Algorithm and Pro-China Influence Networks Indoctrinate GenZ Users in the United States*, 2024 NETWORK CONTAGION RESEARCH INST. 3, 8–10, 21–22 (2024), https://perma.cc/VK2E-ALGT (finding that anti-China content is less likely to be seen on TikTok, and that TikTok users had significantly more positive views of China.); Wan Li, *Data Privacy and China's "Super App" WeChat*, 12 PENN ST. J. L. INT'L AFF. 70, 77–78 (2024); Jeffrey Knockel, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall & Ron Deibert, *We Chat, They Watch, How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus*, 127 CITIZEN LAB 5, 6 (2020).

China's documented hacking efforts and heists of personal information about U.S. citizens added to the suspicion that China would use TikTok for the same ends.[67] In 2025, U.S. officials learned about another platform, GoLaxy, which had been mining data; this development demonstrates how the use of artificial intelligence allows Chinese companies to mine data from both Chinese and non-Chinese social media and create customized propaganda at a greater scale than before.[68] China has also acquired sensitive datasets about Americans through purchases.[69] These efforts are relevant because they indicate China's broader capabilities and intentions, beyond TikTok. Bulk personal information (stolen, collected, or purchased) improves China's ability to develop detailed profiles on

67. Examples of Chinese hacking targeting U.S. personal data abound; this footnote lists only a few examples.

Salt Typhoon: Salt Typhoon is the name that Microsoft gave to a major hack of telecommunications providers, which Microsoft and the intelligence community assessed originated in China. Congressional Research Service (CRS) reports on Salt Typhoon describe intrusions at U.S. telecom providers that reached systems used to furnish court-approved access for law-enforcement and intelligence investigations. CRS notes Chinese actors "may have sought access to these systems . . . to gain access to presidential candidate communications," with the potential to retrieve unencrypted voice calls and text messages. CHRIS JAIKARAN, CONG. RSCH. SERV., IF12798, SALT TYPHOON HACKS OF TELECOMMUNICATIONS COMPANIES AND FEDERAL RESPONSE IMPLICATIONS 1 (2025); Greg Myre, *China Wants Your Data – And May Already Have It*, NPR (Feb. 24, 2021), https://perma.cc/YMQ3-56SU. Perhaps ironically, among the recent targets of the Salt Typhoon hack were databases maintained to meet telecommunications providers' obligations under FISA. *See* Krouse et al., *supra* note 22; David E. Sanger & Julian E. Barnes, *China's Hacking Reached Deep Into U.S. Telecoms*, N.Y. TIMES (Nov. 21, 2024), https://perma.cc/3SEU-79C8.

Access to U.S. Infrastructure: U.S. and allied cyber agencies have warned that China's state-sponsored actors have maintained access to U.S. aviation, rail, maritime, pipeline, water/sewage, and energy networks, often targeting operational technology assets. *See generally* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, PRC STATE-SPONSORED ACTORS COMPROMISE AND MAINTAIN PERSISTENT ACCESS TO U.S. CRITICAL INFRASTRUCTURE (2024), https://perma.cc/A6XT-PZ4P.

Theft of Personal Information: U.S. indictments and official statements also attribute major thefts of Americans' personal information to China's state-sponsored actors, including: security-clearance files (SF-86 forms) and 5.6 million fingerprints; Equifax records (social security numbers, birth dates, addresses); and the 2015 breach of Anthem, Inc., a health insurer, affecting about 78 million people. Regarding the security files, see generally U.S. DEP'T OF NAVY, FREQUENTLY ASKED QUESTIONS: OPM DATA BREACH (Dec. 9, 2015), https://perma.cc/H73E-6KSF. Regarding Equifax, see Press Release, U.S. Dep't of Just., Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking Into Credit Reporting Agency Equifax (Feb. 10, 2020), https://perma.cc/2Y3B-P2CS; *Chinese Hackers Charged in Equifax Breach*, FED. BUREAU OF INVESTIGATION (Feb. 10, 2020), https://perma.cc/AXT6-GUTN. Regarding Anthem, see Press Release, U.S. Dep't of Just., Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People (May 9, 2019), https://perma.cc/H8CG-CHTT.

68. GoLaxy's software can ingest "tens of millions of pieces of data per day" to build "profiles on individuals" and authentic-seeming AI-generated propaganda. Julian E. Barnes, *China Turns to A.I. in Information Warfare*, N.Y. TIMES (Aug. 6, 2025), https://perma.cc/MZ9B-5LM7.

69. For example, a 2021 report from the National Counterintelligence and Security Center described China's efforts to acquire healthcare data about Americans. This included Chinese investment in U.S. healthcare firms, partnerships with hospitals, and purchases of genomic sequencing companies. NAT'L COUNTERINTELLIGENCE & SEC. CTR., CHINA'S COLLECTION OF GENOMIC AND OTHER HEALTHCARE DATA FROM AMERICA: RISKS TO PRIVACY AND U.S. ECONOMIC AND NATIONAL SECURITY 2 (2021), https://perma.cc/4B3R-KFYU. A 2024 EO noted China's efforts to acquire bulk personal data, the risks of selling bulk data to China and other countries of concern, and placed restrictions on such data transactions. EO 14117, *supra* note 22, §§ 1–2.

people of interest ("micro-targeting"), complementing the manipulation risks identified in the *TikTok* record, such as algorithmic curation and content suppression.[70] That combination strengthens the argument that it is important to prevent China's access to large U.S. social media datasets, and that it is not a speculative risk.

C. Russia's Access to Russian Social Media Company Data

The Russian System for Operative Investigative Activities ("SORM") refers to a technical system for intercepting data from Russian communications providers, along with the legal framework that supports it. SORM-1, which originated in the 1990s, intercepts telephone calls.[71] SORM-2 monitors internet traffic, while SORM-3 allows Russian agencies to view communications across multiple platforms, including calls, Wi-Fi, web traffic, and email.[72] Communications providers are required to create a mechanism for Russian agencies to access the data stored on providers' platforms without needing to request the data from the providers.[73] The 2016 Yarovaya Law updated the requirements for the social media age: it required messenger services, platforms, and forums to store metadata for one year and content information for up to six months within Russia, and mandated that they provide Russian agencies with decryption keys for encrypted messages.[74] While the government agent viewing the intercepted material must

---

70. *See, e.g.*, Anthony H. Cordesman, *From Competition to Confrontation with China: The Major Shift in U.S. Policy*, CTR. FOR STRATEGIC & INT'L. STUD. (Aug. 3, 2020), https://perma.cc/F87J-RLMS (summarizing speeches by national security officials and quoting National Security Advisor Robert O'Brien's statement that China will use bulk data "to target, to flatter, to cajole, to influence, to coerce, and to even blackmail individuals to say and do things that serve the Party's interests. This is 'micro targeting' beyond an advertiser's wildest dreams.").

71. JACLYN KERR, THE RUSSIAN MODEL OF INTERNET CONTROL AND ITS SIGNIFICANCE 4 (2018).

72. James Andrew Lewis, *Reference Note on Russian Communications Surveillance*, CTR. FOR STRATEGIC & INT'L. STUD. (Apr. 18, 2014), https://perma.cc/225E-BW3X.

73. Some observers have described this requirement, which grants the Russian Federal Security Service ("FSB") access to data flows within Russia:

> Each telecom or internet operator is obliged by law to install special software and hardware, called SORM or System for Operative Investigative Activities, which allows FSB to gain access to users' personal data. In this case, information is accessed by special services without the knowledge of telecom or internet companies. The FSB officer simply enters the command through the SORM control panel, which is connected to the operator's servers.

Evgeni Moyakine & Alexander Tabachnik, *Struggling to Strike the Right Balance Between Interests at Stake: The 'Yarovaya', 'Fake News' and 'Disrespect' Laws as Examples of Ill-Conceived Legislation in the Age of Modern Technology*, 40 COMPUTER L. & SEC. REV. 105512, *5 (2021) (footnote omitted).

74. Federal'nyi± Zakon RF No. 374-FZ, o Vnesenii Izmeneniy v Federal′nyi± Zakon "O Protivodeystvii terrorizmu" i Otdel′nye Zakonodatel′nye Akty Rossii±skoi± Federatsii v Chasti Ustanovleniya Dopolnitel′nykh Mer Protivodeystviya Terrorizmu i Obespecheniya Obshchestvennoy Bezopasnosti [Federal Law of the Russian Federation No. 374-FZ on Amendments to the Federal Law "On Counteracting Terrorism" and Certain Legislative Acts of the Russian Federation Regarding the Establishment of Additional Measures to Counter Terrorism and Ensure Public Safety], SOBRANIE ZAKONODATEL'STVA ROSSII±SKOI± FEDERATSII [SZ RF] [Russian Federation Collection of Legislation] 2016, No. 28, art. 4558. Article 15 of the law contains new requirements that enable intelligence agencies to access social network and internet communication data. *Id.* The law applies to any "organizer of information dissemination on the Internet." *Id.* (translated from Russian by Apple Translate). According to

obtain a judicial warrant to access the data available through SORM, multiple sources indicate that this is rarely done in practice and does not serve as a reliable check on agencies' ability to access the information.[75]

The primary social networking company in Russia is VK Group, which controls the email provider Mail.ru and the formerly independent social networks VKontakte and Odnoklassniki.[76] The case of VKontakte is illustrative of the trend toward State control over data held by Russian social media companies. VKontakte's co-founder and original CEO, Pavel Durov, left the company in 2014 as Russian authorities pressed VKontakte to provide user information.[77] VKontakte was sold to Mail.ru, and the resulting company was named VK Group.[78] As of 2025, VK Group's goal is to create a service like WeChat that provides one stop for all communication needs.[79] This would also enhance VK Group's surveillance potential. At present, user information and the contents of communications on VKontakte are easily available to Russian authorities.[80]

Moyakine and Tabachnik, "The procedure for examining, storing and processing personal data is far from clear, it is not defined who the authorities are that are authorized to get access to the information in question and which bodies supervise the exercise of these powers." Moyakine & Tabachnik, *supra* note 73, at 6.

75. Before the Yarovaya Law was implemented, the European Court of Human Rights reviewed the warrant requirements and other procedural safeguards under the SORM legal framework at the time. *See* Zakharov v. Russia, 2015-VIII Eur. Ct. H.R. 205, 222–225. These included the Operational Search-Activities Act of 1995 and the Code of Criminal Procedure for accessing telecommunications data. *See id*. They concluded, "Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and abuse." *Id*. at 296. Other authors were skeptical that the agents apply for warrants at all. Valeriy Akimenko & Keir Giles, *Russia's Cyber and Information Warfare*, 15 ASIA POLICY 67, 73 (2020); Moyakine & Tabachnik, *supra* note 73, at 5. The federal agent "should get an eavesdropping warrant, but he is not obliged to show it to anyone." Andrei Soldatov, Investigative Journalist and Founder of Agentura.Ru, Russia's Communications Interceptions Practices (SORM), Presentation at Hearing Before European Parliament Subcommittee on Human Rights (Jan. 22, 2014).

76. Gregory Asmolov, *Russian Social Media Logic: Between the East and the West*, KNIGHT FIRST AMEND. INST. (May 6, 2021), https://perma.cc/3ENM-LYC4.

77. Durov stated he was asked by the FSB to provide data on organizers of Ukraine's Euromaidan movement. Oliver Poole, *Russia, Sliding Downhill After Sochi*, *in* 2014 GLOB. INFO. SOC'Y WATCH 206, 208 (Alan Finlay ed.), https://perma.cc/S38E-RPQF. Durov continued to develop Telegram, an encrypted messaging app, which is based in Dubai. Joshua Berlinger & Anna Chernova, *A Russian Elon Musk with 100 Biological Children: Meet Pavel Durov*, CNN BUSINESS (Aug. 27, 2024), https://perma.cc/T7ND-ZF8D.

78. Ivan Chermousov, *Why Mail.ru Group was Renamed to VK*, ROS. GAZ. (Oct. 18, 2021) (Russian State media), https://perma.cc/V84C-RAUD.

79. Philipp Dietrich, *Russia Purports to Build a Fully Controlled, State-Run IT Ecosystem,* GER. COUNCIL ON FOREIGN REL. (Nov. 17, 2023), https://perma.cc/2DK6-QN8Q.

80. Morgan Meaker, *How the Kremlin Infiltrated Russia's Facebook*, WIRED (June 1, 2022), https://perma.cc/J9MN-QRZ7. Russia's efforts to gather personal data extend beyond Russian companies, illustrating that while Russia may have greater access to data managed by Russian companies, it is also seeking information elsewhere. For example, the FSB is collecting and analyzing data from WeChat, including logins, contact lists, and chat archives, to monitor individuals who might be communicating with Chinese intelligence. Despite Russia's ties to China, this highlights inevitable suspicion regarding digital surveillance between countries. Aaron Krolik & Paul Sonne, *Russian Intelligence Says It Collects WeChat Data. What Does That Mean?*, N.Y. TIMES (June 7, 2025), https://perma.cc/ZWJ3-7VS9. This tension can be viewed as an example of an emerging "security dilemma" between China and Russia. *See supra* note 14 and *infra* note 82.

In sum, the United States, China, and Russia have all developed legal and technical mechanisms that enable expansive access to data collected through domestically headquartered social media platforms. In the United States, however, such access is subject to statutory and judicial checks, including Foreign Intelligence Surveillance Court review and congressional oversight, that do not exist in China or Russia. This surveillance does not stop at national borders. State access to these platforms' data affects the rights of users and the security of States around the world. In response, States have adopted a range of strategies to mitigate this threat. The following section classifies these responses along a spectrum.

III. A SURVEY OF RESPONSES: BAN, DIVESTITURE, AND DATA PRIVACY REGULATION

This section identifies examples of State responses to social media threats that fit into three categories: bans, divestiture mandates, and data privacy regulation. This section presents the authors' observations about each category.

The concepts of "offensive" and "defensive" actions are helpful in analyzing each response.[81] For example, comprehensive privacy regulation applies neutrally and is therefore more likely to appear "defensive" to other States, promoting the status quo. On the other hand, bans and divestiture requirements might appear "offensive," seeking a new benefit or pushing the envelope, drawing a reaction. A State forcing divestiture may characterize it as a defensive risk mitigation strategy, while the State subject to the action may characterize it as an offensive ban or seizure. A State imposing a blanket ban may characterize it as defensive, but a State subject to the ban may characterize it as an offensive denial of market access and impose countersanctions.[82] The categorization of responses achieved in this article makes it easier to see why certain actions may be perceived as offensive.

A. Complete Ban

This subsection examines the "complete ban" as a policy instrument. A ban is a government measure that bars access to, or distribution and maintenance of, specified social media applications within national networks and app marketplaces. This subsection uses three cases: Ukraine's 2017 blocking of Russian platforms; India's post-2020 prohibitions on TikTok and hundreds of other Chinese apps; and China's long-standing exclusion of most foreign platforms through its censorship and cybersecurity regime. These cases were included because,

81. For an explanation of offensive and defensive actions, see *supra* note 13. Actions interpreted as offensive may be more likely to elicit reactions from other States. However, actions taken for defensive reasons can also spur responses from rivals, in part due to "[S]tates' uncertainty and fears about each other's present and future intentions." Tang, *supra* note 14, 592–93.

82. For a discussion of the security dilemma as applied to State actions in cyberspace, see Woodrow Wilson Center, *The Cybersecurity Dilemma*, YOUTUBE (Mar. 23, 2017), https://perma.cc/9B3P-MHVE (e.g., beginning at 6:15). Ben Buchanan, interviewed in this video, explores the concept further in his book, cited *supra* note 12. For further exploration of the security dilemma, see Tang, *supra* note 14, and Yoav Gortzak, Yoram Haftel & Kevin Sweeney, *Offense-Defense Theory: An Empirical Assessment*, 49 J. CONFLICT RESOLUTION 67 (2005).

although adopted under different circumstances, they share the common feature of completely preventing access to specific social media platforms.

There are many instances of bans beyond those discussed here. For example, TikTok, although just one platform, has garnered many complete or partial bans. In 2024, at least 38 countries had imposed some form of restriction on TikTok, citing national security and intelligence law concerns.[83] Some countries, such as India and Nepal, instituted full bans of the application for all users, motivated by geopolitical tensions or perceived threats to "social harmony."[84] Authoritarian regimes like Iran and North Korea have included TikTok among the suite of global social platforms permanently blocked from general access. Others have restricted the app's use in certain cases.[85] In 2025, Australia banned ten social media platforms for children under 16 to protect children's mental well-being and prevent exposure to harmful content.[86]

Bans may be imposed for many reasons, but this section focuses on the countries' cited national security or counterintelligence concerns. Suppression of internal dissent and a desire to control the narrative are also powerful motivations.[87] It is beyond the scope of this article to analyze these reasons, e.g., to provide thoughts on which

83. *See* Anna Gordon, *Here's All the Countries With TikTok Bans as Platform's Future in U.S. Hangs In Balance*, TIME (Apr. 25, 2024), https://perma.cc/4AY5-FAX8; *TikTok's Expanding Ban: A Global Snapshot of Countries Taking Action*, FUTURE (Jan. 20, 2025), https://perma.cc/GP43-4RAK.

84. *See*, *e.g.*, Mariko Oi, *Nepal Bans TikTok Citing Disruption to Social Harmony*, BBC (Nov. 13, 2023), https://perma.cc/GE59-H8B4. Nepal later lifted its ban. Anil Giri, *Nepal Lifts Its Ban on TikTok*, KATHMANDU POST (Aug. 23, 2024), https://perma.cc/4NUR-S7AT.

85. For instance, Canada, Belgium, and the United Kingdom have restricted the app's use on government-issued devices, citing the need to protect sensitive information from foreign surveillance. *See* Gordon, *supra* note 83. The Government of Canada also ordered TikTok Technology Canada Inc. to shut down its offices after a national security review under the Investment Canada Act, which permits the government to block foreign investments deemed harmful to national security. However, it did not ban the platform. Innovation, Sci. and Econ. Dev. Canada, *Government of Canada Orders the Wind Up of TikTok Technology Canada, Inc. Following a National Security Review Under the Investment Canada Act*, GOV'T OF CAN. (Nov. 6, 2024), https://perma.cc/S88L-PWNZ. In many European countries, such as Austria, Denmark, and Ireland, similar bans have been imposed on civil servants' work devices, and the European Union's institutions have followed suit. Jordan banned the app following the death of a police officer during a protest. Senegal and Somalia cited the app's use in spreading subversive or terrorist content for their bans. Azerbaijan and Armenia both temporarily blocked TikTok during periods of armed conflict. Some bans are framed as efforts to protect cultural or moral values. Afghanistan, Bangladesh, and Kyrgyzstan cited harm to youth or societal degradation. In other cases, such as Indonesia, commercial violations were the driving force; TikTok Shop was banned for allegedly breaching e-commerce regulations. Gordon, *supra* note 83.

86. *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth) (Austl.); Helen Livingstone, *Australia Has Banned Social Media for Kids Under 16. How Will It Work?*, BBC (Dec. 9, 2025), https://perma.cc/FEP5-CKN9. Children under 16 are banned from accessing Facebook, Instagram, Snapchat, Threads, TikTok, X, YouTube, Reddit, Kick, and Twitch. *Id.*

87. For example, restrictions on China's internet, in place for over 30 years, are a tool of social control. For an analysis of China's reasons for controlling access to the internet, see Jordan J. Foley, *China's Authoritarian Grip: How China Reinforces Social Control, Cultivates a Climate of Fear, and Minimizes Dissent*, AIR FORCE J. INDO-PACIFIC AFFS. (Nov. 15, 2023), https://perma.cc/YUC7-JK6X. According to Foley, the Chinese Communist Party's "paramount concern" related to the internet is "potential political instability." "Internet sovereignty," or stopping "unwanted information at its borders" leads to suppression of dissent.

concerns about foreign surveillance are really covers for suppression of internal dissent. The authors maintain that we can analyze how these tools addressed States' counterintelligence and counter-manipulation objectives, even if the restrictions had other goals as well.

1. Examples from Ukraine, India, and China

Since May 2017, Ukraine has blocked VK Group platforms (including VKontakte, Mail.ru, and Odnoklassniki), as well as the Russian-owned portal Yandex, due to their storage of user data in Russia and the influence of Russian security services over their operations.[88] The policy must be understood in the context of the ongoing armed conflict between Ukraine and Russia, which has heightened concerns about disinformation and espionage. This ban followed VK's documented compliance with Russian intelligence requests during the 2014 protests against Russian influence in Ukraine and reflects a national effort to cut off Russian influence channels.[89]

The ban proved effective: by 2021, only 7% of Ukrainians still used VKontakte.[90] In contrast, in Russian-occupied Ukrainian territories, authorities have blocked platforms such as Facebook, Instagram, YouTube, Viber, and even Google since 2022, while Russian platforms like VK and Odnoklassniki remain fully accessible.[91] In 2020, nearly 46% of Ukrainians supported the Ukrainian VKontakte ban, marking an increase from an approval rating of around 20% in June 2017.[92] Human rights advocates have warned that these measures, in addition to lacking full effectiveness, have raised rule-of-law concerns, curtailed Ukrainians' digital rights, particularly freedom of expression, and have also imposed economic and informational costs.[93] The former representative of the Ukrainian parliament's commissioner for human rights protested that "blocking access to sites without a court decision is not allowed" under Ukrainian law.[94]

---

88. Olha Snopok, *VKontakte with the Occupiers: The Russian Propaganda Machine in the Temporarily Occupied Territories*, UKRAINSKA PRAVDA (May 17, 2023), https://perma.cc/P8KF-EZ7Y.

89. These protests are known in Ukraine and the West as the Revolution of Dignity or the Euromaidan movement. *See id*. *See also* AFP, *Pavel Durov Left Russia After Being Pushed Out*, ECON. TIMES (Apr. 22, 2014), https://perma.cc/QC6P-AVVE ("Durov said this month he had came under pressure from the Russian security services to reveal data on VKontakte users, and that his refusal led to his losing his stake in the company."); Ingrid Lunden, *Durov, Out For Good From VK.com, Plans A Mobile Social Network Outside Russia* (Apr. 22, 2014), https://perma.cc/54GB-EWAY (further explaining the tension surrounding Durov's departure). As discussed *supra* note 77, VK founder Pavel Durov was pressured to provide data on Ukrainian Euromaidan organizers, and he left the company because of this. Soon after, the Mail.ru Group took control of the platform. By 2015, control had passed to Russian oligarch Alisher Usmanov, a supporter of the war in Ukraine. Snopok, *supra* note 88.

90. Snopok, *supra* note 88.

91. *Id.*

92. Daryna Antoniuk, *Ukraine Prolongs Ban on Russian Websites VKontakte, Odnoklassniki Until 2023*, KYIV POST (May 16, 2020), https://perma.cc/5PHS-2RNH. *See also* Alec Luhn, *Ukraine Blocks Popular Social Networks as Part of Sanctions on Russia*, GUARDIAN (May 16, 2017), https://perma.cc/TET6-48DK ("Of more than 11,000 respondents to an online poll on the UNIAN site on Tuesday afternoon, 66% said they were 'categorically against' the ban of VK, Yandex and other Russian sites.").

93. Olga Kyryliuk, *Should Ukraine Drop Sanctions Against Russian Tech Companies?*, FREEDOM HOUSE (Dec. 2019), https://perma.cc/AX85-FF9S.

94. Alec Luhn, *Ukraine Blocks Popular Social Networks as Part of Sanctions on Russia*, GUARDIAN (May 16, 2017), https://perma.cc/KKU4-QGZE.

In June 2020, India banned TikTok along with dozens of other Chinese apps following a deadly border clash with China.[95] India cited national security and privacy concerns, stating that the decision to ban the apps was to protect citizens' data privacy and that the apps were "stealing and surreptitiously transmitting users' data in an unauthorized manner to servers outside India."[96] The Indian government's concerns closely mirror those expressed by U.S. officials (detailed in Section II.B *supra*) regarding Chinese laws compelling data access by State authorities. At the time, India had around 200 million TikTok users, making it the app's largest market outside China.[97] India's ban also formed part of a broader strategy to reduce Chinese economic influence; it has banned over 500 Chinese apps to date.[98] The Indian government has not offered extensive explanation regarding the legal or cybersecurity rationale behind its bans, although legal analysts identified that the bans are likely authorized under Section 69A of India's Information Technology Act of 2000.[99] This section empowers the Indian government to control and monitor digital communications in the interest of national security and public order.[100] The shutdown sparked disappointment from TikTok users in India, many of whom were economically dependent on the platform and felt the TikTok algorithm was more localized to Indian cultural content than U.S.-based social media algorithms.[101] The ban, in a way, traded one country's

95. Krutika Pathi, *Here's What Happened When India Banned TikTok*, PBS (Apr. 24, 2024), https://perma.cc/RDW5-NVNB; Hannah Ellis-Petersen, *India Bans TikTok After Himalayan Border Clash with Chinese Troops*, GUARDIAN (June 29, 2020), https://perma.cc/DXG6-TLMU.

96. Pathi, *supra* note 95; Ellis-Petersen, *supra* note 95.

97. Pathi, *supra* note 95; Ellis-Petersen, *supra* note 95.

98. Ellis-Petersen, *supra* note 95.

99. Justin Sherman, *The Problem with India's App Bans*, ATLANTIC COUNCIL (Mar. 27, 2023), https://perma.cc/VJ7C-4KZS.

100. Section 69A is titled, "Power to issue directions for interception or monitoring or decryption of any information through any computer resource." It authorizes the central or state governments to order the interception, monitoring, or decryption of information transmitted or stored on any computer resource, if necessary for purposes such as national defense, public order, or preventing crime. Agencies executing such orders must follow prescribed procedures and record their reasons in writing. Intermediaries (such as internet providers or platforms) are legally required to assist, and noncompliance is punishable by up to seven years in prison and a fine. Section 69A allows the central government to block public access to online content under similar grounds, such as protecting sovereignty or public order. Orders must follow prescribed procedures, and intermediaries that fail to comply can face up to seven years of imprisonment and a fine. Section 69B permits the central government to authorize government agencies to monitor and collect internet traffic data for cyber security purposes, including preventing malware or other computer contaminants. Intermediaries must provide full cooperation or risk penalties of up to three years' imprisonment and a fine. The Information Technology Act, 2000, § 69.

101. Alex Travelli & Suhasini Raj, *What Happened When India Pulled the Plug on TikTok*, N.Y. TIMES (Mar. 22, 2024), https://perma.cc/QC2E-BZYM (featuring a video interview with Ulhas Kamathe, who became famous "by devouring chicken platters while murmuring 'chicken leg piece'"). Mr. Kamathe lost his seven million TikTok viewers, but eventually managed to rebuild his following on YouTube, Instagram, and Facebook. *Id. But cf.* Mihir Sharma, *Life After TikTok Isn't So Fun. Just Ask India*, BLOOMBERG (May 1, 2024), https://perma.cc/X6CN-6Y4Z (arguing that the alternatives to TikTok, such as YouTube and Instagram Reels, were not as good at promoting creator content and making money for creators).

surveillance for another's: Meta's Instagram and Alphabet's YouTube became the most popular platforms.[102]

India's response reflects the significance of the responding State's relationship with the surveilling State: India's geopolitical alignment and shared democratic institutions with the United States make U.S.-based platforms politically less threatening than Chinese ones, even if both retain broad data-collection capabilities. India may also have been less concerned about retaliation in its trading relationship with China than in its trading relationship with the United States.[103] Nevertheless, China noted its disapproval: in June 2020, the Ministry of Foreign Affairs said that Beijing was "strongly concerned," and urged India to protect the rights of foreign investors.[104] China characterized India's ban as economic discrimination.[105] China asserts that India's bans violate World Trade Organization ("WTO") rules; China continues to raise this at the WTO, most recently in June 2025.[106]

China's "Great Firewall," its system of internet censorship and surveillance, blocks access to virtually all major foreign social media platforms, including Facebook, Instagram, and YouTube.[107] China began imposing legal restrictions on internet access in the 1990s; while many laws and regulations currently

---

102. Thomas Germain, *The Ghosts of India's TikTok: What Happens When a Social Media App Is Banned*, BBC FUTURE (Dec. 6, 2024), https://perma.cc/S4JE-AJEV (interviewing an Indian tech policy analyst and news site founder about Chinese response).

103. In 2024, the United States was India's largest trading partner, and China was India's second-largest trading partner. However, the dynamics of the two relationships were different: India enjoyed a trade surplus with the United States but had a trade deficit with China, likely leading it to prioritize its relationship with the United States. The U.S. imposition of steep tariffs on India in 2025 may alter this dynamic, pushing it more toward China. Alisa Sachdev & Dan Strumpf, *Why India Increasingly Needs China, and Vice Versa*, BLOOMBERG (Oct. 27, 2025), https://perma.cc/JQ6C-CBGY ("The two sides traded $127 billion of goods last year, although most of that — $109 billion — were Chinese exports to India."). *See also* Sushant Singh, *How Vulnerable is India to Chinese Economic Coercion*, U.S. INST. FOR PEACE (June 16, 2025), https://perma.cc/9SDQ-K23U ("India's overall trade with the United States is comparable to its trade with China but India enjoys a substantial $36.7 billion trade surplus with the United States.").

104. *See China "Strongly Concerned" After India Bans 59 Chinese Apps*, INDIA TODAY (June 30, 2020), https://perma.cc/2BEC-WW4P.

105. *China Opposes Discriminatory Actions by India Against Chinese Firms*, REUTERS (Jan. 27, 2021), https://perma.cc/2R58-PFWP.

106. Kamya Pandey, *Five Years On, China Still Opposing India's Chinese Apps Ban at WTO*, MEDIANAMA (Sep. 11, 2025), https://perma.cc/5HXG-Q5YZ.

107. The New York Times described the Great Firewall as:

> a combination of blocking just about any foreign website you can think of and providing an information environment that reinforces what China's government and the Chinese Communist Party say about the world. The controls are comprehensive. A huge government bureaucracy monitors online activity, and an army of volunteers report content to be censored and help spread positive messages about government initiatives.

Shira Ovide, *Copying China's Online Blockade*, N.Y. TIMES (Mar. 1, 2021), https://perma.cc/L38W-4CQW (interview with Paul Mozur). Websites including chinafirewalltest.com test whether a particular site is blocked in China. In September 2025, Facebook, Instagram, and YouTube were blocked in China, although X was not. *China Firewall Test*, VIEW DNS, https://perma.cc/93FW-6CEG (last visited Sep. 25, 2025) (Facebook), https://perma.cc/C5JW-86ZB (last visited Sep. 25, 2025) (Instagram), https://perma.cc/T75N-DKU8 (last visited Sep. 25, 2025) (YouTube), https://perma.cc/35MX-KD97 (last visited Sep. 25, 2025) (X).

support the Firewall, the Cybersecurity Law provides foundational authority.[108] The Firewall enjoys some support among Chinese citizens, although true feelings may be hard to measure.[109] These restrictions are part of a strategy to maintain control over online discourse.[110] While the official rationale often cites the need to preserve cultural values, the Great Firewall also reflects longstanding concerns about foreign surveillance—particularly in response to revelations of U.S. intelligence operations and data collection through American tech platforms.[111] China directs its population to use apps over which it has control, such as WeChat, Weibo, and Douyin.[112]

2. Lessons from this Approach

The States that have implemented full social media bans often do so in moments of geopolitical tension. Ukraine's measures came amid invasion and ongoing war, and India's followed a deadly border clash. China's prohibitions reflect enduring rivalry and distrust toward Western powers. For a State seeking to preserve working and positive diplomatic or economic relations, a complete ban may not prove worthwhile.

---

108. Article 6 of a 1996 order required international networking to go through government channels and set the stage for the current Firewall. Zhonghua Renmin Gongheguo Jisuanji Xinxi Wangluo Guoji Lianwang Guanli Zanxing Guiding (中华人民共和国计算机信息网络国际联网管理暂行规定) [Provisional Management Regulations for the International Connection of Computer Information Networks of the People's Republic of China] (promulgated by the St. Council, Feb. 1, 1996), Order No. 195, art. 6, 1996:4 GAZETTE OF THE STATE COUNCIL OF THE PEOPLE'S REPUBLIC OF CHINA 102, 103, *translated in* Rogier Creemers, *Provisional Management Regulations for the International Connection of Computer Information Networks of the People's Republic of China*, DIGICHINA (Feb. 1, 1996), https://perma.cc/HXR6-PVSW.

Article 50 of the Cybersecurity Law directs government agencies to monitor internet communications, including those from outside China, and "where they discover the publication or transmission of information which is prohibited by laws or administrative regulations," direct network operators to block transmission. Cybersecurity Law, *supra* note 63, art. 50.

109. Steve Guo & Guangchao Feng, *Understanding Support for Internet Censorship in China: An Elaboration of the Theory of Reasoned Action*, 17 J. CHINESE POL. SCI. 33, 34 (2011) (discussing reactions to the "chain of firewalls, accompanied by vigorous rationalization of their implementation" in young people and noting that "[d]espite numerous inconveniences censorship entails, it has not precluded Chinese, especially the young, from vowing support for various restrictions authorities impose on domestic and foreign political websites").

110. *See* Foley, *supra* note 87.

111. While China has stated various rationales for the Firewall, since the extent of American surveillance came to light in 2013, rhetoric has increasingly included "cybersecurity" as a rationale. *See, e.g.*, Samantha Hoffman, *Ensuring Comprehensive State Security in the "Ideological Battleground" Online*, JAMESTOWN FOUND. (Nov. 16, 2015), https://perma.cc/952S-9VQE ("Since early 2014, the Communist Party has regularly emphasized that 'without cyber security there is no state security.'"). For more discussion of the rationale behind the Great Firewall, see KIERAN GREEN, ANDREW SPROTT, ED FRANCIS, BRIAN LAFFERTY, HARTLEY WISE, MOLLY HENRY, GRACE FAERBER & FRANK MILLER, CTR. FOR INTEL. RSCH. & ANALYSIS, CENSORSHIP PRACTICES OF THE PEOPLE'S REPUBLIC OF CHINA 8–14 (2024), https://perma.cc/ABS4-YQV3. *See also* Elizabeth Economy, *The Great Firewall of China: Xi Jinping's Internet Shutdown*, GUARDIAN (June 29, 2018), https://perma.cc/T2HD-SJ7R.

112. Li Yuan, *To Cover China, There's No Substitute for WeChat*, N.Y. TIMES (Jan. 9, 2019), https://perma.cc/JD9S-J89Q.

Summary Comparison Chart of Three National Bans

Country	Platform(s) Banned	Stated Rationale	Suspected Legal/Policy Basis	Strategic Objective	Effectiveness/ Consequences
Ukraine	VK Group platforms (VKontakte, Odnoklassniki, and Mail.ru), search engine Yandex	National security; influence of Russian intelligence; data stored in Russia	Presidential decree in context of ongoing war between Russia and Ukraine	Curtail Russian propaganda and surveillance	By 2021, VK use dropped to 7% in Ukraine; ban remains in place; contrast in occupied territories where Russian apps dominate; initially unpopular
India	TikTok (and over 500 Chinese apps)	Data privacy and national security; unauthorized data transfers; post-border clash with China	Section 69A of the Information Technology Act of 2000	Reduce Chinese digital and economic influence and surveillance	Effective platform removal; shift of users to U.S. alternatives
China	Facebook, Instagram, YouTube, and others	National security; ideological control; foreign surveillance concerns	National Cybersecurity Law, censorship regime ("Great Firewall")	Maintain State control over information; protect regime legitimacy; respond to U.S. surveillance	Near-total exclusion of Western platforms; promotion of domestic alternatives (WeChat, Weibo)

Another observation of the ban approach is that it is relatively simple and can be implemented quickly. As observed in the cases of Ukraine banning VKontakte, India banning TikTok, and China banning U.S. social media, bans are often effective at moving most users off the target platform.[113]

Bans can have harmful consequences. Users can circumvent bans using virtual private networks ("VPNs").[114] Bans disrupt the livelihoods of creators and businesses that rely on them for income or communication, as seen in India. Bans

113. Even the threat of a ban can induce compliance from social media companies. For example, Sarah Wynn-Williams characterizes Facebook's 2014 decision to censor pages in Russia as a preemptive decision to avoid a ban. SARAH WYNN-WILLIAMS, CARELESS PEOPLE 159 (2025). Sheryl Sandberg's email to Mark Zuckerberg, quoted in the book, also illustrates the multi-dimensional and iterative nature of the problem: "This is certainly small compared to potential China requests and will be noted by them too." *Id.* Another example of preemptive actions to avoid regulation is TikTok's transfer of U.S. user data to Oracle servers located in the United States and TikTok's plans to manage U.S. user data by a subsidiary staffed only by U.S.-based employees. As seen in Section III.B *infra*, these actions proved insufficient to avoid a divestiture requirement. Perault, *supra* note 63.

114. *See*, *e.g.*, *Why are VPNs Getting Slower in China?*, ECONOMIST (Aug. 22, 2024), https://perma.cc/Y2M7-FFDN; Evie Steele, *China's VPN Usage Nearly Doubles Amid Internet Censorship*, VOA (Feb. 15, 2024), https://perma.cc/GD5E-RVFP.

impede free speech since users are no longer free to express themselves on their chosen platforms. In countries with First Amendment-like protections for free speech, blanket bans without a divestment option may face legal challenges.[115]

Additionally, targeting one platform at a time is a piecemeal strategy that fails to address the broader structural risks, since new platforms will continue to emerge. For example, the Ukrainian ban of VKontakte did not address the threat of Russian infiltration over Telegram, and Ukraine later had to take further action, banning Telegram from government devices.[116] In India, users switched to Meta's platforms, becoming more susceptible to U.S. monitoring.[117] The trade- and security-driven nature of the Indian ban underscores that who is doing the surveilling matters and not merely the technical capacity for data collection.

Unilateral actions could also provoke mirror-image proposals and litigation elsewhere in the world, with uncertain implications for global commerce.[118] Bans intended to be "defensive" (protecting the population from surveillance) might be perceived as "offensive" or escalatory since they single out certain providers for disparate treatment.[119] In a game-theory framework, a ban is a high-salience move that changes the opponent's incentives to retaliate in other stages of the game (trade, tech, investment).[120] For example, in 2024, one commentator predicted "a far greater chance a US TikTok ban would spark a trade war" than India's TikTok ban.[121] Because U.S.-China interdependence enables cross-domain retaliation, a US TikTok ban could be a higher-cost move than India's ban. The prediction about U.S. TikTok restrictions becoming part of a greater trade war proved prophetic: in 2025, the sale of TikTok was negotiated amid broader trade talks in response to U.S.-imposed tariffs.[122]

B. Divestiture Requirement

As seen in the previous section, a ban simply prevents access to the platform of concern. By contrast, a State implementing a divestiture requirement threatens

115. The Supreme Court applied intermediate scrutiny in *TikTok Inc. v. Garland* because the law was content neutral. The Court observed, "[PAFACAA] directly regulates ByteDance Ltd. and TikTok, Inc. only through the divestiture requirement. . . . Petitioners, for their part, have not identified any case in which this Court has treated a regulation of corporate control as a *direct* regulation of expressive activity or semi-expressive conduct." TikTok Inc. v. Garland, 604 U.S. 56, 68 (2025). This analysis suggests the Court may view a direct ban on a specific platform differently from the divestiture requirement.

116. Olena Harmash, *Ukraine Bans Official Use of Telegram App over Fears of Russian Spying*, REUTERS (Sep. 20, 2024), https://perma.cc/95PY-D4XQ.

117. Germain, *supra* note 102.

118. For instance, in Ireland, politician Simon Harris has recently called for consideration of a social media ban for children under 16, referencing Australia's pioneering legislation as a model. Ellen Fitzpatrick, *Simon Harris Says Social Media Ban for Teenagers Under 'Serious Consideration' amid 'Ticking Time Bomb' Alert*, SUN (IRELAND) (May 9, 2025), https://perma.cc/8S3A-PJ4G.

119. Offensive and defensive actions are further discussed in notes 13 and 81 *supra*.

120. The "security dilemma," in which defensive moves may be perceived as offensive, is further discussed *supra* notes 82 and 14.

121. Germain, *supra* note 102.

122. Max Zahn, *TikTok, Toy Prices and More: What's at Stake in US-China Trade Talks*, ABC NEWS (Oct. 29, 2025), https://perma.cc/MC3Y-5ZGV.

to ban the platform unless the owners of the platform sell the platform (or at least the part of the platform operating within the State). Although a divestiture requirement will result in a ban if no buyer is found, recognizing divestiture requirements as a separate category prevents the misconception that divestiture requirements always equate to bans.

Attorney David Dorfman, Chief Counsel and Deputy Staff Director for the House Select Committee on the Chinese Communist Party in 2024 and one of the lead drafters of PAFACAA, explained the difference between a ban and a divestiture requirement. According to Mr. Dorfman, TikTok tried to portray PAFACAA as a ban, although it was not:

> TikTok tried desperately to deceive its users into believing the TikTok divestiture law was a ban. Congress didn't fall for it, and on a 9-0 basis, neither did the Supreme Court. The Act is not only entirely consistent with longstanding foreign ownership restrictions in U.S. law, but in fact even narrower, since it only applies in the case of four specifically designated countries and particular apps determined to present a grave national security harm.[123]

The United States has employed two mechanisms to compel divestitures of social media companies when foreign ownership in those companies poses a national security threat. In this section, the article examines a statutory divestiture requirement (PAFACAA) and an executive-driven process (CFIUS). These examples are chosen because they represent two paths to impose divestiture; both have been used to regulate social media companies. This section concludes with an examination of some lessons from these approaches.

1. Statutory Requirement: PAFACAA

The United States' push to remove TikTok from ByteDance's control began as an executive-driven process, stalled, was revived by Congress's passage of unprecedented legislation, and reverted to an executive-driven process as the Trump Administration negotiated a deal creating a new venture to control TikTok's U.S. user data.[124] The PAFACAA case study illustrates both the challenges and the potential of a divestiture requirement.

a. Road to PAFACAA

In 2017, ByteDance acquired Musical.ly and merged its users into TikTok, a global version of its Chinese app Douyin.[125] TikTok's rapid U.S. growth drew scrutiny from CFIUS, which in 2020 found national security risks in the

123. Interview with David Dorfman, Chief Counsel/Deputy Staff Director, House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party (May 11, 2025) (virtual).

124. *See* Petition for Review, *supra* note 1; 15 U.S.C. § 9901 note; EO 14352, *supra* note 4; *TikTok USDS Announcement*, *supra* note 7.

125. Petition for Review, *supra* note 1, at 8.

platform.[126] This scrutiny arose largely in response to China's legal framework described in Section II.B *supra*, which permits extensive State access to data held by companies like ByteDance.[127] President Trump then ordered ByteDance to divest TikTok's U.S. operations, citing data collection; ties to the Chinese Communist Party; and the potential for surveillance, blackmail, and disinformation.[128] TikTok obtained an injunction blocking the order.[129]

In 2021, President Biden revoked the Trump-era divestment order and pursued negotiations with ByteDance to protect user data.[130] The talks stalled.[131] Evidence continued to emerge that Americans' data was being accessed in China.[132] Congress passed PAFACAA in April 2024, mandating that U.S. providers stop offering access to TikTok unless ByteDance divested by January 19, 2025.[133] In advance of the PAFACAA vote, ODNI released its annual assessment outlining national security threats, noting that "TikTok accounts run by a PRC [People's Republic of China] propaganda arm reportedly targeted candidates from both political parties during the U.S. midterm election cycle in 2022."[134] Also in the lead-up to PAFACAA, members of Congress expressed concern over China's access to American data and ability to manipulate the American public using that information.[135]

b. Passage of PAFACAA and the Supreme Court Decision

PAFACAA requires that U.S. companies cease distributing and providing internet services to "foreign adversary controlled applications."[136] It designates

126. *Id*. at 44–49.

127. *Id*. at 45–48.

128. 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, Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020) (ordering divestment following CFIUS recommendation) [hereinafter EO 13942]; Regarding the Acquisition of Musical.ly by ByteDance Ltd., 85 Fed. Reg. 51,297 (Aug. 14, 2020) (more specific order targeting the corporate transaction) [hereinafter ByteDance Order].

129. TikTok Inc. v. Trump, No. 1:20-cv-02658 (D.D.C. Sep. 27, 2020) (order granting preliminary injunction).

130. Protecting Americans' Sensitive Data from Foreign Adversaries, Exec. Order No. 14,034, 86 Fed. Reg. 31,423 (June 9, 2021).

131. Drew Harwell, *TikTok Offered an Extraordinary Deal. The U.S. Government Took a Pass*., WASH. POST (May 29, 2024), https://perma.cc/P5AM-59FA (TikTok proposed allowing federal officials to select the board of directors for its U.S. operations, granting the government veto power of its new hires, hiring a U.S. contractor affiliated with the Department of Defense to monitor its source code, and allowing federal authorities a "kill switch" to shut down the app if they determined it posed an ongoing risk).

132. Emily Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed from China*, BUZZFEED NEWS (June 17, 2022), https://perma.cc/43RM-DZ9K.

133. 15 U.S.C. § 9901 note §§ 2(a)(1), 2(a)(2)(A).

134. OFF. OF THE DIR. FOR NAT'L INTEL., ANNUAL THREAT ASSESSMENT 12 (2024); Mallory Culhane, *The Chinese Government Is Using TikTok to Meddle in Elections, ODNI Says*, POLITICO (Mar. 11, 2024), https://perma.cc/AUW2-D2RE.

135. *See*, *e.g*., *TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms: Hearing Before the H. Comm. on Energy and Commerce*, 118th Cong. 35 (Mar. 23, 2023) (statements of Reps. Cathy McMorris Rodgers, John Sarbanes, Jay Obernolte, John Curtis, and Lisa Blunt Rochester) [hereinafter *TikTok Congressional Hearing*].

136. 15 U.S.C. § 9901 note § 2(a)(1).

any application operated by ByteDance or TikTok as "foreign adversary controlled" and empowers the executive to make additional designations.[137] The requirement was to take effect 270 days after PAFACAA was enacted.[138] However, PAFACAA exempted applications executing a qualified divestiture, and it allowed the President to extend implementation by ninety days if there is "significant progress" toward a qualified divestiture.[139]

The Supreme Court upheld the law in *TikTok Inc. v. Garland*. The Court concluded that the law only required intermediate First Amendment scrutiny because the divestment requirement was facially content-neutral.[140] It survived that scrutiny because it served a compelling, content-neutral national security interest: preventing a foreign adversary from gathering sensitive personal information from over 170 million U.S. users.[141] The Court acknowledged the risks posed by China's trove of U.S. user information.[142]

c. Implementation of PAFACAA

The day after the Court's ruling, TikTok ceased operations.[143] Apple and Google removed the app from their stores.[144] The platform remained offline until then-President-elect Trump posted on Truth Social, pledging to extend the law's implementation period.[145] Following that assurance, TikTok resumed service.[146] On January 20, 2025, President Trump delayed enforcement of the requirement that ByteDance divest from TikTok, citing the need to prevent an abrupt shutdown and allow time for further negotiations.[147]

---

137. *Id.* § 2(g)(3).

138. *Id.* § 2(a)(2)(A).

139. *Id.* § 2(a)(3).

140. TikTok Inc. v. Garland, 604 U.S. 56, 70–73, 77 (2025).

141. *Id.* at 76.

142. *See*, *e.g.*, *id.* at 74 ("Access to such detailed information about U.S. users, the Government worries, may enable China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.") (internal quotations and citations omitted); *id.* ("Chinese law enables China to require companies to surrender data to the government, making companies headquartered there an espionage tool of China.") (internal quotations and citations omitted); *id.* ("TikTok can access any data stored in the user's contact list, including names, contact information, contact photos, job titles, and notes.") (internal quotations and citations omitted); *id.* at 75 ("Even if China has not yet leveraged its relationship with ByteDance Ltd. to access U.S. TikTok users' data, petitioners offer no basis for concluding that the Government's determination that China might do so is not at least a reasonable inference based on substantial evidence.") (internal quotations and citations omitted).

143. Sapna Maheshwari, Madison Malone Kircher, Eli Tan & Meaghan Tobin, *TikTok Goes Dark in the U.S.*, N.Y. TIMES (Jan. 18, 2025), https://perma.cc/QHU3-FBTY.

144. Jonathan Vanian, *Apple, Google Remove TikTok from Stores as App Halts Service in U.S.*, CNBC (Jan. 18, 2025), https://perma.cc/G4XU-CD8G.

145. David Shepardson, *TikTok Restores US Service After Trump Says "We Have to Save It,"* REUTERS (Jan. 20, 2025), https://perma.cc/J3SY-2KJK.

146. *Id.* Apple and Google restored TikTok to app stores in February 2025. Bobby Allyn, *TikTok is back on the Apple and Google app stores*, NPR (Feb. 13, 2025), https://perma.cc/T6U4-9VEF.

147. Application of Protecting Americans from Foreign Adversary Controlled Applications Act to TikTok, Exec. Order No. 14,166, 90 Fed. Reg. 8,611 (Jan. 20, 2025) [hereinafter EO 14166].

President Trump's pause did not come as a surprise; he expressed skepticism about PAFACAA in 2024 despite earlier support for action against TikTok.[148] President Trump's reluctance to immediately ban the app was likely due to its popularity among American users, including his supporters and conservative influencers.[149] Additionally, Trump stated his administration required time to assemble U.S.-based investors.[150]

The long pause in PAFACAA enforcement highlighted that statutory divestiture requirements rely on enforcement by the President, especially in an administration with an expansive view of presidential powers. In letters to tech companies telling them they would not be in violation of the law if they provided internet services to TikTok, Attorney General Pamela Bondi argued that the President had the ability to determine whether to enforce the law.[151] Bondi claimed that PAFACAA should not be interpreted as infringing on the President's responsibilities for national security and foreign policy as granted in Article II of the Constitution.[152] Some commentators assessed that by repeatedly delaying implementation of PAFACAA beyond the ninety-day extension period, and by informing tech companies that the law would not be enforced, the President had unconstitutionally suspended a law passed by Congress.[153] On the other hand, the President's delays went unchallenged, and PAFACAA has no mechanism to compel the President to enforce the law. This experience shows that the effect of a statutorily imposed divestiture requirement can vary widely from administration to administration, giving the President the option to order divestment rather than mandating divestment.

d. The Brokered TikTok Deal

On September 25, 2025, President Trump announced that he had determined that a proposed "framework agreement"—which had not been made public—would meet the requirements of PAFACAA if implemented.[154] Trump signed an

148. John Garrison, *'I Got to Use It': Donald Trump's Evolution from TikTok Foe to a Fan*, USA TODAY (Jan. 22, 2025), https://perma.cc/DAQ5-Q4HD.

149. Colleen McClain, *Fewer Americans Now Support TikTok Ban, See the Platform as a National Security Threat Than in Spring 2023*, PEW RSCH. CTR. (Mar. 25, 2025), https://perma.cc/TE4T-UFVP; Lisa Friedman & Sapna Maheshwari, *How Donald Trump Went from Backing a TikTok Ban to Backing Off*, N.Y. TIMES (Dec. 28, 2024), https://perma.cc/57GU-NRKL; Taylor Lorenz, *These Influencers Helped Get Trump Elected. Now They're Ready to Party*, ROLLING STONE (Jan. 20, 2025), https://perma.cc/C33T-PQBA. Influential Republican donors, including Jeff Yass, who is an investor in ByteDance, may have also changed President Trump's mind on the matter. Morgan Phillips, *From Ban to Embrace: Trump's Evolution on TikTok and What Comes Next*, FOX BUS. (Aug. 25, 2025), https://perma.cc/JU84-M5TE.

150. EO 14166, *supra* note 147.

151. *See, e.g.*, Letter from Attorney General Pamela Bondi to Katherine Adams, Senior Vice President & General Counsel, Apple Inc., Re: Enforcement of the Protecting Americans from Foreign Adversary Controlled Applications Act (Apr. 5, 2025), https://perma.cc/F67B-BD33.

152. *Id.*

153. Alan Z. Rozenshtein, *The TikTok Ban that Wasn't*, BROOKINGS (June 20, 2025), https://perma.cc/LE2D-V4KL; The New York Times Editorial Board, *Opinion: Trump Is Letting TikTok (and China) Win*, N.Y. TIMES (Aug. 8, 2025), https://perma.cc/AS69-ES5Q.

154. *TikTok Framework Fact Sheet*, *supra* note 5.

EO delaying enforcement of PAFACAA until January 23, 2026 to allow the deal to conclude.[155] The EO announced that "TikTok's United States application will be operated by a newly established joint venture based in the United States" and that ByteDance will own less than 20% of the joint venture.[156] The White House also announced that U.S. TikTok data will be stored in the United States by Oracle.[157] According to the White House, the new joint venture will license TikTok's content recommendation algorithm from ByteDance, but the algorithm will be "retrained and operated" in the United States.[158] The White House claimed the version of the app available in the United States will be interoperable with the international version; U.S. users will be able to view content from outside the United States, and vice versa.[159]

ByteDance signed a deal implementing the "framework" in December 2025, and in January 2026, ByteDance and investors formed a new entity called TikTok USDS Joint Venture LLC ("TikTok USDS").[160] According to a press release by TikTok USDS, ByteDance owns 19.9% of TikTok USDS, with the remaining 80.1% held by a consortium led by Oracle, the private equity firm Silver Lake, and MGX, an investment firm controlled by the government of Abu Dhabi.[161] Each of these major stakeholders owns 15% of TikTok USDS; the announcement listed other investors but did not specify how much of TikTok USDS they own.[162] TikTok USDS represented that it will protect U.S. user data in Oracle's U.S. cloud environment, and that it will "retrain, test, and update the content recommendation algorithm" in the Oracle environment using U.S. user data under a security program that was designed to meet industry standards and third-party

155. EO 14352, *supra* note 4, § 3(a).

156. *Id.* § 1; *see also TikTok Framework Fact Sheet*, *supra* note 5.

157. *TikTok Framework Fact Sheet*, *supra* note 5. White House Spokesperson Karoline Leavitt stated that the data "will be stored securely in the United States without access from China." WHITE HOUSE, *Press Secretary Karoline Leavitt Briefs Members of the Media*, at 23:30 (The White House, Sep. 22, 2025), https://perma.cc/58SF-ATM2 [hereinafter *Leavitt Briefing*].

158. The White House did not provide many details about ByteDance's agreement to let the U.S. entity use the algorithm. An unnamed White House official described the arrangement as a license. Emmett Lindner & Lauren Hirsch, *U.S.-run TikTok to License Algorithm, White House Says*, N.Y. TIMES (Sep. 22, 2025), https://perma.cc/PG89-HN5D. The September 2025 EO claimed, "The divestiture puts the operation of the algorithms and code, as well as content-moderation decisions, under the control of the new joint venture." EO 14352, *supra* note 4, § 2(b)(iii)(B). Leavitt stated that the algorithm will be "outside of ByteDance's control." *Leavitt Briefing*, *supra* note 157, at 23:50.

159. *Leavitt Briefing*, *supra* note 157, at 24:00.

160. Shepardson, *supra* note 6; *TikTok USDS Announcement*, *supra* note 7; Bonny Chu, *TikTok Avoids US Ban by Finalizing Historic Trump-backed American Majority Ownership Deal*, FOX BUS. (Jan. 22, 2026), https://perma.cc/3PW4-4L85.

161. *TikTok USDS Announcement*, *supra* note 7. These three investors were referred to as "managing investors." *Id. See also* Everson, *supra* note 7 (discussing Abu Dhabi's ownership of MGX).

162. *TikTok USDS Announcement*, *supra* note 7. The other investors named in the press release were: The Dell Family Office (Dell CEO Michael Dell's private investment firm); Vastmere Strategic Investments, LLC, an affiliate of Susquehanna International Group, an early ByteDance investor; Alpha Wave Partners; the investment firm Revolution; Merrit Way, LLC; Via Nova; Virgo LI, Inc., described as the "investment arm of a foundation established by Yuri and Julia Milner in support of science"; and NJJ Capital. *Id. See also* Katie Malone, *The Firm Owned by Pennsylvania's Richest Man Is Now Co-leading US TikTok*, TECHNICAL.LY (Jan. 23, 2026), https://perma.cc/PUE8-G3BS.

audit and certification expectations.[163] At the same time, the press release stated that "TikTok global's U.S. entities"—not TikTok USDS—will continue to manage "global product interoperability and certain commercial activities, including e-commerce, advertising, and marketing," preserving an operational role for the global TikTok corporate structure in core revenue functions.[164] In addition, U.S. users encountered updated privacy terms; these terms expanded collection and use of data, including users' precise location (if users enable location services), logging of interactions with TikTok's AI tools, and broader use of data for targeting ads outside of the TikTok app.[165] Because the underlying deal and day-to-day operational arrangements were not made public, and the parties disclosed few specifics about the business relationship among TikTok USDS, global TikTok, and ByteDance, lawmakers have called for congressional scrutiny of whether the structure satisfies PAFACAA's requirement that U.S. operations not maintain a prohibited "operational relationship" with "formerly affiliated entities that are controlled by a foreign adversary."[166]

The various announcements about the birth of TikTok USDS left unanswered questions about how the new app will prevent Chinese access to user data and remove Chinese influence over the content shown to U.S. users. While White House Press Secretary Karoline Leavitt stated that the licensed recommendation algorithm will be "operated" by TikTok USDS, it is unclear how this arrangement

163. *TikTok USDS Announcement*, *supra* note 7. The announcement contained no new information about the terms of the arrangement under which TikTok USDS receives permission from ByteDance to use the algorithm. News reports and commentators continued to describe the arrangement as a "license." *See* Emmett Lindner, *There's a New American TikTok. What Does That Mean for You?*, N.Y. TIMES (Jan. 22, 2026), https://perma.cc/6XB8-JF2D; Kenton Thibaut, *TikTok's New Ownership Structure Doesn't Solve Security Concerns for Americans*, ATL. COUNCIL (Jan. 27, 2026), https://perma.cc/683P-C47B.

164. *TikTok USDS Announcement*, *supra* note 7. TikTok CEO Shou Chew has a seat on the TikTok USDS board of directors. *Id*. The press release stated that the safeguards will also "cover CapCut and Lemon8," other ByteDance-affiliated apps, but did not specify what "cover" means or the relationship between TikTok USDS and these apps. *Id*. TikTok USDS released a website that has longer biographies of its directors and its chosen corporate leaders. *TikTok USDS Joint Venture LLC*, TIKTOK USDS JV, https://perma.cc/8R78-V4SC (last visited Jan. 26, 2026).

165. Reece Rogers, *TikTok Is Now Collecting Even More Data About Its Users. Here Are the 3 Biggest Changes*, WIRED (Jan. 23, 2026), https://perma.cc/36GM-D4LY. *Compare Privacy Policy*, TIKTOK (Jan. 22, 2026), https://perma.cc/8S7X-HVPU [hereinafter *New Privacy Policy*], *with Privacy Policy*, TIKTOK (Aug. 19, 2024), https://perma.cc/6KK7-M7H8.

166. 15 U.S.C. § 9901 note § 2(g)(6)(B) (specifically prohibiting "any cooperation with respect to the operation of a content recommendation algorithm or an agreement with respect to data sharing"); David Shepardson, *US Lawmakers Say TikTok Joint Venture Deal Needs Scrutiny from Congress*, REUTERS (Jan. 23, 2026), https://perma.cc/U7W6-JGRQ; Moolenaar, *supra* note 8. Representative Raja Krishnamoorthi, a primary author of PAFACAA, objected in September 2025 to the lack of information that had been released about the deal, saying, "If a deal has been struck, the details need to be shared with Congress. President Trump will be judged based on the answer to one question: whether the deal complies with the law to keep TikTok available to U.S. users, but without CCP control. Under the TikTok Divestiture Law, the new American TikTok can have no operational relationship with ByteDance." Raja Krishnamoorthi, *Krishnamoorthi Responds to Latest Reporting on a Potential TikTok Deal*, H. SELECT COMM. ON STRATEGIC COMPETITION BETWEEN THE U.S. & THE CHINESE COMMUNIST PARTY (Sep. 22, 2025), https://perma.cc/G7KC-PH5E.

would work in the long term,[167] such as whether the licensing and interoperability requirements would give ByteDance influence over TikTok USDS,[168] and whether the ByteDance-controlled worldwide TikTok platform will receive information about U.S. users as those users interact with content from outside the United States.[169] The announcements made one thing clear, however: PAFACAA's divestiture requirement resulted in a deal driven by the White House.[170]

2. CFIUS-Mandated Divestiture

PAFACAA is not the only example of mandated divestiture; CFIUS may review foreign investments to determine whether they pose a risk to national security, suspend those investments, and recommend that the President mandate divestment.[171] CFIUS is chaired by the Secretary of the Treasury; statutory members include the Secretaries of Homeland Security, Commerce, Defense, State, Energy, and Labor, the Attorney General, and the DNI.[172] CFIUS may review transactions resulting in foreign control of a U.S. business or investments in companies involved in critical infrastructure, critical technologies, or sensitive personal data, even if they do not result in foreign control of those businesses.[173] A 2018 statute expanded CFIUS's authority to review minority foreign investments in U.S. companies if they involve access to

---

167. *Leavitt Briefing*, *supra* note 157, at 23:50.

168. Marc Short, a former Trump Administration official, and Michael Sobolik, a former legislative assistant to Senator Ted Cruz, noted that the deal "leaves the core of TikTok's technology under Chinese control." Marc Short & Michael Sobolik, *TikTok Is a National Security Threat. This Is What the Trump Administration Needs to Do*, FOX NEWS (Sep. 25, 2025), https://perma.cc/SJ8P-RH74. While the technical details are not known at this time, it is easy to imagine how ByteDance may retain a significant amount of influence over U.S. users. For example, to remain interoperable with the international version of TikTok, the U.S. version of TikTok may need to receive updates to the algorithm from ByteDance. It is not clear whether the licensing involves a one-time transfer of code that will be permanently forked, or whether it involves future updates. Additionally, since it will be feeding content to the U.S. version of the app from overseas users, ByteDance could still exert a great degree of influence over what is shown.

169. Writing about Project Texas, TikTok's earlier plan to keep user data in Texas under Oracle supervision, Matt Perault noted that data would need to flow out of the United States when a user messages someone internationally or posts a video globally. He noted that the solution would be "a version of TikTok that walled off U.S. users from the rest of the world." Perault, *supra* note 63.

170. During a press conference announcing the framework, President Trump and Vice President J.D. Vance acknowledged that the deal was driven by the Administration. Vice President Vance stated, "We really couldn't have done this without the President actually ushering this deal over the finish line." WHITE HOUSE, *President Trump Signs Executive Orders*, at 3:13 (The White House, Sep. 25, 2025), https://perma.cc/CH6F-QC2H. President Trump stated, "J.D. was very much involved in charge of it." *Id*. at 2:54.

171. 50 U.S.C. § 4565.

172. *Id*. § 4565(k)(2). The DNI and Secretary of Labor are nonvoting. The President may appoint additional members; as of December 2025, the Office of the U.S. Trade Representative and Office of Science & Technology Policy are members of CFIUS. *CFIUS Overview*, DEP'T OF TREAS., https://perma.cc/Z6AT-XFGZ.

173. 50 U.S.C. § 4565(a)(4)(B). The term "control" means the power, direct or indirect, whether exercised or not exercised, to determine, direct, or decide important matters affecting an entity, subject to regulations prescribed by the Committee. *Id*. § 4565(a)(3). Real estate transactions in ports or near sensitive military installations are another category of transaction that may be reviewed. *Id*. § 4565(a)(4)(B)(ii).

technical information, board representation, or decision-making influence.[174] The Committee may suspend a "proposed or pending" transaction while the transaction is under review and may recommend that the President suspend or prohibit the transaction.[175]

Rising tensions between the United States and China during President Trump's first administration impacted cross-border tech investment, particularly in sectors involving sensitive data.[176] Increased CFIUS scrutiny led to divestitures, including the forced sales of Grindr by Beijing Kunlun and PatientsLikeMe by iCarbonX, both due to concerns over foreign access to sensitive personal data. Grindr and PatientsLikeMe can be defined as social media platforms, like TikTok, Facebook, or VK.[177]

In 2017, Chinese genomics firm iCarbonX and New York-based Invus Group invested $100 million in PatientsLikeMe to integrate patient-reported data with advanced machine learning.[178] However, in April 2019, CFIUS raised national security concerns about Chinese access to PatientsLikeMe's sensitive health data, prompting iCarbonX to divest.[179] In June 2019, U.S. insurance company UnitedHealth Group acquired PatientsLikeMe.[180] The acquisition was successfully completed, and in 2021, PatientsLikeMe raised funds again, but none of the new investors drew scrutiny from CFIUS.[181] In 2025, the company announced that it joined Fuze Healthcare.[182] The many investments and changes in ownership after CFIUS involvement exemplify a company surviving an adverse CFIUS decision and also show the fluidity of company ownership.

Chinese mobile gaming company Beijing Kunlun Tech Co. Ltd ("Kunlun") acquired a majority stake in Grindr, one of the largest LGBTQ+ dating apps, in 2016, and bought out the company in 2018.[183] It failed to submit its transactions

174. Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Pub. L. No. 115-232, § 1701, 132 Stat. 1636. The Treasury Department Fact Sheet provides a concise explanation of FIRRMA's changes and the implementing regulations. *See generally* DEP'T OF TREAS., FACT SHEET: FINAL CFIUS REGULATIONS IMPLEMENTING FIRRMA (Jan. 13, 2020), https://perma.cc/4235-4GL2.

175. 50 U.S.C. § 4565(d), (l). Parties to covered transactions may initiate review through notices or declarations; CFIUS can also review transactions not submitted by the parties. *Id.* § 4565(b)(1)(C), (b)(1)(D), (b)(1)(H).

176. Gina Chon, *Breakingviews - U.S.-PRC Tensions Upend Tech Funding Supply Chain*, REUTERS (June 4, 2019), https://perma.cc/U89G-W2JK.

177. *See, e.g.*, *Investor Relations*, GRINDR, https://perma.cc/M5KK-2TEH ("Grindr is the number 1 social network for the LGBTQ+ community."); Catherine Arnott Smith & Paul J. Wicks, *PatientsLikeMe: Consumer Health Vocabulary as a Folksonomy*, AMERICAN MED. INFORMATICS ASSOC. ANN. SYMP. PROC., Nov. 2008, at 682, 683, https://perma.cc/M2FG-H9QF ("PatientsLikeMe is an online social networking community allowing members to track their progress with clinical scales, share information, and learn more about their condition.").

178. Matthew Herper, *PatientsLikeMe, Forced by U.S. to Ditch Chinese Investor, Sold to UnitedHealth Group*, STAT (June 24, 2019), https://perma.cc/X6WN-SAXN.

179. *Id.*

180. *Id.*

181. *Patient Health Network PatientsLikeMe Raises $26 Million*, MERCOM CAP. GRP. (Feb. 10, 2021), https://perma.cc/R3K3-C8S4.

182. Krysta S., *PatientsLikeMe Joins the Fuze Health Family*, PATIENTSLIKEME (June 2025), https://perma.cc/VJ2J-C28U. According to Fuze's website, it has an address in Atlanta. *Contact Us*, FUZEHEALTH, https://perma.cc/29WB-CV4W.

183. *Id.*

to CFIUS.[184] CFIUS review resulted in Kunlun divesting from Grindr due to national security concerns over the app's sensitive user data, including private messages and HIV status.[185] In May 2020, CFIUS approved the $620 million sale of Grindr by Kunlun to a U.S.-based investor group, San Vicente Acquisition LLC.[186] The sale was successful, but few details were publicly disclosed about San Vicente. In a demonstration of how divestment transactions are not always a clean break from the original owners, Reuters reported that a founder of San Vicente was a business partner of Kunlun's founder and that Kunlun offered San Vicente favorable financing terms.[187]

This kind of retrospective scrutiny and intervention is an example of a non-legislative divestiture mechanism. These were successful divestments, kept services available, and received little public notice or pushback. On the other hand, broad statutory permission for the executive branch to force divestiture may be used overexpansively by an empowered President.[188] Since CFIUS members are all political appointees, committee actions and recommendations are prone to influence by the President's agenda.[189] Litigants have successfully challenged expansive uses of CFIUS or other executive-driven economic powers, as shown by TikTok's 2020 litigation to block the implementation of the CFIUS-driven divestiture requirement by the first Trump Administration.[190] Another facet of

184. *Id.*

185. *Id.*

186. Echo Wang, *China's Kunlun Says U.S. Approves Sale of Grindr to Investor Group*, REUTERS (May 29, 2020), https://perma.cc/YY7L-6S4L.

187. Echo Wang, Alexandra Alper & Chibuike Oguh, *Exclusive: Winning Bidder for Grindr Has Ties to Chinese Owner*, REUTERS (June 2, 2020), https://perma.cc/JJ96-K2VG. Grindr's new buyers took the app public in 2022; as of 2025, two of the original shareholders, the Singapore-based Raymond Zage and the U.S.-based James Lu, own 60% of the company. Jessica Tan, *The Inside Story of How a Former Hedge Fund Star Made His First Billion on Grindr*, FORBES (Oct. 9, 2025), https://perma.cc/BU24-ZBPA; Kritika Lamba, *Grindr Ends Talks on $3.46 Billion Take-Private Bid over Financing Uncertainty*, REUTERS (Nov. 24, 2025), https://perma.cc/N29B-HED7.

188. For example, in 2025, President Trump used another economic measure, the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701–1708, to impose widespread tariffs. The Court of Appeals for the Federal Circuit ruled that President Trump had exceeded his authority, a matter that was before the Supreme Court as of January 2026. V.O.S. Selections, Inc. v. Trump, 149 F.4th 1312, 1334 (Fed. Cir. 2025) (IEEPA did not include the ability to tax or impose tariffs, and presidentially imposed tariffs triggered the major questions doctrine).

189. 50 U.S.C. § 4565(k)(2) (stating the members of CFIUS).

190. TikTok Inc. v. Trump, 507 F. Supp. 3d 92, 97, 115 (D.D.C. 2020) (suit to enjoin bans and other EO actions); TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 86 (D.D.C. 2020) (granting emergency injunction). These cases challenged EO 13942, *supra* note 128, and the order requiring divestment from TikTok (ByteDance Order, *supra* note 128). The order requiring divestment cited CFIUS as authority, while EO 13942 additionally cited IEEPA, 50 U.S.C. §§ 1701–1708, as authority. IEEPA prohibits restrictions on personal communications and informational materials. In TikTok v. Trump, 507 F. Supp. 3d at 109, the D.C. District Court determined that TikTok content and user data fall within these protected categories. For a discussion of the use of IEEPA to regulate social media, see Bernard Horowitz & Terence Check, *TikTok v. Trump and the Uncertain Future of National Security-Based Restrictions on Data Trade*, 13 J. NAT'L SEC. L. & POL'Y 61, 67–71 (2022) (explaining why IEEPA, traditionally used to sanction regimes involved in terrorism, weapons proliferation, and other serious threats, may not be an appropriate tool for addressing bulk collection of ordinary USP data).

complete executive control over the CFIUS process is that it is even easier for the popularity of a product to lead to presidential inaction; with no statute forcing the President's hand, the TikTok CFIUS process languished until the passage of PAFACAA.[191]

3. Lessons from this Approach

a. Burning Bridges for a "Credible Commitment" to Prevent Adversary Access

As of January 2026, twenty-one months after PAFACAA's passage, it appears that the law will achieve its immediate goal: removing a hoard of American user data from the direct control of a Chinese-owned company. The law achieved this despite a change in administration, a change in public opinion regarding the law, the popularity of the platform, a marketing campaign by the owners, and the initial reluctance of the owners to come to a negotiated solution. The earlier CFIUS-driven examples also succeeded in removing the platforms from problematic owners while keeping those platforms alive. The strategy of requiring parties to reach a deal involving a sale, but not pre-defining the terms of the deal, incentivized the sellers and purchasers to find mutually beneficial terms. It remains to be seen whether the TikTok sale will reduce China's ability to conduct espionage or influence operations online.

ByteDance's partial divestiture from TikTok convinced at least some American decision-makers that the platform no longer posed a threat. The contrast between this result and TikTok's earlier, unsuccessful efforts to keep U.S. user data under third-party supervision in the United States is an example of the "credible commitment" problem, in which bridges need to be burned to bring credibility to a player's commitment and induce desired responses from other players.[192] In 2023, TikTok announced "Project Texas," a proposal under which TikTok planned to open a subsidiary in the United States to handle U.S. user data; that subsidiary's data would be kept in the United States on Oracle Cloud, which would monitor data flows to ensure that there are no improper transfers of data abroad.[193] However, lawmakers did not believe TikTok's assurances that ByteDance (and China) would not be able to access U.S. user data stored in

191. *See* One Country Project's Hot Dish, *TikTok: What You Need to Know* (Apple Podcasts, Feb. 5, 2025), https://perma.cc/R5SE-8CUK (Heidi Heitkamp interview with David Dorfman, discussing the delays in the CFIUS-driven response to TikTok, leading Congress to take action with PAFACAA, at 19:00). *See also* Courtney Fingar, *Congress' TikTok Bill Tries to Fix What CFIUS Failed to Do Years Ago*, FORBES (Mar. 20, 2024), https://perma.cc/3H5E-EPGU.

192. The "credible commitment" problem is further discussed in note 19 *supra*.

193. Perault, *supra* note 63; Matt Perault & Samm Sacks, *Project Texas: The Details of TikTok's Plan to Remain Operational in the United States*; LAWFARE (Jan. 26, 2023), https://perma.cc/P3Z6-85ZR (CFIUS would be allowed to approve all appointees to the U.S. subsidiary's board); *About Project Texas*, TIKTOK, https://perma.cc/A5PE-28PS (last visited Dec. 30, 2025). To pursue Project Texas, TikTok created a U.S.-based entity called TikTok U.S. Data Security Inc. to manage U.S. user data, a structure which bore a close resemblance to the later-established TikTok USDS Joint Venture. *What Is USDS and How Is It Governed?*, TIKTOK, https://perma.cc/UX5Y-LSRP (last visited Dec. 29, 2025).

Texas.[194] In other words, shifting the data's storage location while retaining ownership did not sufficiently constrain ByteDance to bring credibility to its commitment; Congress still perceived the bridge to U.S. user data as intact. In the eyes of Congress, only by selling a majority stake could ByteDance sufficiently "burn the bridge" to U.S. user data.

b. Flexibility to Adapt to Threats and Allow for Negotiation

One key lesson of the divestiture approach is its flexibility: if a targeted platform is sold to a non-adversary entity, the ban may be avoided and user access preserved. If there is enough political will or economic incentive to separate the platform from the perceived threat, the platform need not be banned. This conditional mechanism could theoretically be used to preempt future threats. Unlike a single-platform ban, PAFACAA applies not only to TikTok but also to any "foreign adversary controlled application" that the President determines presents a threat to national security.[195] This helped the bill's defenders respond to criticism that PAFACAA was only directed at TikTok.[196] Given that general data protection legislation has been notoriously difficult to pass in the United States, a narrow divestiture bill was arguably Congress's best option.[197] The bill's authors crafted legislation addressing the root cause of the concern, which improved on an outright ban, and which was upheld by the Supreme Court.

Mr. Dorfman argued that PAFACAA's divestiture requirement improved on a ban:

> A notable and underappreciated feature of the statute is that divestiture functions as a perpetual—and not a one-time—compliance option. In other words, even if ByteDance initially allowed the restrictions to take effect, a later decision to

194. *TikTok Congressional Hearing*, *supra* note 135 (statement of Rep. Jay Obernolte) ("I don't believe that it is technically possible to accomplish what TikTok says it will accomplish through Project Texas. I just think that there are too many back doors through that process to allow that to be possible."); *id.* (statement of Rep. Frank Pallone) ("I still believe that the Beijing Communist government will still control and have the ability to influence what you do."); *id.* (statement of Rep. Angie Craig) ("You know, clearly, in the 3-plus hours you have been before us today, what you are saying about Project Texas just doesn't pass the smell test. My constituents are concerned that TikTok and the Chinese Communist Party are controlling their data and seeing our own vulnerabilities.").

195. 15 U.S.C. § 9901 note § 2(g)(3).

196. For example, TikTok argued in its petition to the Court of Appeals for the D.C. Circuit that the law violated its right to equal protection and constituted an unconstitutional bill of attainder since it singled out ByteDance by name for adverse treatment. Petition for Review of the Constitutionality of the Protecting Americans from Foreign Adversary Controlled Applications Act at 56–62, TikTok Inc. v. Garland, 122 F.4th 930 (D.C. Cir. 2024) (No. 24-1113). The D.C. Circuit rejected these arguments, writing, "By naming TikTok in the Act, the Congress ensured TikTok-related risks were addressed promptly. Simultaneously creating a generally applicable framework gave the Executive a tool to address similar risks that may come to light in the future." TikTok Inc. v. Garland, 122 F.4th 930, 966 (D.C. Cir. 2024).

197. The longstanding gridlock on federal general data privacy legislation is detailed in CAMERON F. KERRY, JOHN B. MORRIS, JR., CAITLIN T. CHIN & NICOL E. TURNER LEE, BRIDGING THE GAPS: A PATH FORWARD TO FEDERAL PRIVACY LEGISLATION, BROOKINGS INST. (2020), https://perma.cc/TC3P-QLM6.

> execute a qualified divestiture would remove those restrictions and permit full restoration of service. The existence of such a regulatory pathway for reinstating an application upon compliance is decidedly different from a 'ban'.[198]

c. Perception of Unfair Targeting and Burdens on Speech

Divestiture has its limitations. It is a reactive, case-by-case approach, requiring individual designation of each platform as adversary-controlled. This leads to a perception of unfairness.[199] TikTok's Chief Executive Officer, Shou Chew, alluded to a double standard in a 2023 House Energy & Commerce hearing, where he faced combative questions. He maintained that TikTok was not an outlier, referencing the 2018 revelations that the consulting firm Cambridge Analytica harvested Facebook data and arguing, "American social companies don't have a good track record with data privacy and user security."[200] Similar to an outright ban, the act of singling out a particular platform may be viewed by the platform and the platform's home country as offensive or provocative rather than defensive.[201] An affected country or company may decide to frame the action in offensive terms for strategic reasons; for example, in order to argue against the divestiture mandate, demand concessions in other areas, or retaliate.

Moreover, as the Supreme Court recognized even while upholding PAFACAA, a divestiture requirement targeting a specific platform is a restriction on the platform users' speech, although permissible under the circumstances.[202] Requiring the divestiture interferes with Americans' ability to choose which companies' products to utilize to publish and receive information.[203] It also interferes with American

---

198. David Dorfman, Email to authors (Dec. 21, 2025).

199. The Final Service, *Regulating Big Tech: Is TikTok Still on the Clock?* (Apple Podcasts, Sep. 18, 2023, at 28:00), https://perma.cc/C4E4-VAXL [hereinafter Final Service Podcast] (host noting that it is ironic for Congress to regulate TikTok's "potential misdeeds given the terrible state of online privacy already" and saying, "They're singling out TikTok for a widespread sin, it seems to me . . . can they really go to war with one provider?").

200. Dara Kerr, *Lawmakers Grilled TikTok CEO Chew for 5 Hours in a High-Stakes Hearing About the App*, NPR (Mar. 23, 2023), https://perma.cc/GP54-S9SR (Chew was "pointing to the Cambridge Analytica scandal where Facebook users' personal data was used for political advertising.").

201. Offensive and defensive actions are discussed in notes 13 and 81 *supra*; the "security dilemma" is discussed in notes 82 and 14 *supra*.

202. *See* TikTok Inc. v. Garland, 604 U.S. 56, 69 (2025) (noting that an "effective ban on a social media platform with 170 million U.S. users certainly burdens those users' expressive activity in a non-trivial way" and assuming without deciding that "regulation of a non-expressive activity that disproportionately burdens those engaged in expressive activity triggers heightened review"); *id*. at 74–78 (upholding the divestiture-backed prohibition under intermediate scrutiny).

203. In 1965, the Supreme Court invalidated a statute that impeded U.S. citizens' access to foreign Communist propaganda. Lamont v. Postmaster General, 381 U.S. 301, 305 (1965). The statute required the Postmaster General to hold unsealed Communist propaganda from abroad until the addressee affirmatively requested it. *Id*. at 302. The Court determined this would deter some addressees from receiving the material, impeding their First Amendment rights. *Id*. at 307. George Wang explains how the "right to receive information," even Communist propaganda, applies to TikTok:

> *Lamont* stands for the proposition that Americans have a right to receive information and ideas from abroad. In the digital age, that means a right to access the social media platforms and discursive

companies' speech—in the case of PAFACAA, this includes the speech of TikTok's American subsidiary and of companies enabling access to TikTok.[204] Additionally, if the designated company cannot find a suitable buyer within the prescribed timeline, the law defaults to a ban—triggering some, but not all, of the legal, technical, and political challenges associated with outright prohibition. The possibility that TikTok would be banned, and the burdens on speech associated with the requirement that ByteDance divest from TikTok, led some scholars to argue that PAFACAA and *TikTok v. Garland* "mark[] a low point for the First Amendment."[205] Even though the law was deemed constitutional, it came at a cost to certain constitutional rights.[206]

d. Handing Power to the President

As compared to a privacy statute containing standards of general applicability, such as GDPR, CFIUS and PAFACAA increase the President's control over American companies. Both statutes grant the President broad discretion to require divestment and to determine when a deal mitigates threats to national security. This was evident in the President's decision to suspend PAFACAA's ban for over a year and to take a central role in negotiating the sale of TikTok.[207] The Trump Administration similarly exercised discretion under the CFIUS statute to condition the Japanese company Nippon Steel's purchase of U.S. Steel on Nippon's guaranteeing the U.S. President a "golden share" in Nippon's U.S. operations; this allows the President to disapprove consequential management decisions.[208]

---

communities of their choosing—even when those speech environments are organized or curated by foreign entities. A ban on TikTok deprives citizens of their right to engage with their preferred social media—along with all the attendant information, ideas, and views that the platform carries.

Xiangnong (George) Wang, *Listeners' Rights in the Time of Propaganda: The Story of Lamont v. Postmaster General*, KNIGHT FIRST AMEND. INST. (Feb. 14, 2025), https://perma.cc/A4BQ-L9K8.

204. *See TikTok,* 604 U.S. at 81 (Sotomayor, J., concurring in part and concurring in the judgment) (PAFACAA "plainly imposes" a burden on speech and association because it "bars any entity from distributing TikTok's speech in the United States, unless TikTok undergoes a qualified divestiture" and "prohibits TikTok from collaborating with certain entities," even if ByteDance divests).

205. Anupam Chander, G.S. Hans & Edward Lee, *TikTok v. Garland Opens the Door to Global Censorship*, LAWFARE (Feb. 6, 2025), https://perma.cc/6H56-FBBJ.

206. The Takings Clause of the Fifth Amendment states: "nor shall private property be taken for public use, without just compensation." U.S. CONST. amend. V. In addition to the First Amendment rights to freedom of speech, press, and association, some have suggested that PAFACAA could infringe on TikTok creators' Fifth Amendment rights. If a ban were to become effective, these creators' accounts would be "taken" by the government without compensating the creators for the value of the account (e.g., followers). *See* Bridget Gilchrist, *TikTok Bans: A Takings Clause Blunder?*, U. CHI. L. REV. ONLINE (May 12, 2025), https://perma.cc/T6PB-JPXU.

207. For an analysis of the Trump Administration's involvement in assembling the investors to buy TikTok, see Alexandra Levine & Kurt Wagner, *Trump's TikTok Deal Puts the White House in the Driver's Seat*, BLOOMBERG (Oct. 13, 2025), https://perma.cc/QHW9-DMGG. For a discussion of how PAFACAA enabled the President to choose purchasers, see David Frum, *Trump's Dodgy Plan for TikTok*, ATLANTIC (Oct. 11, 2025), https://perma.cc/S6GC-PBB6.

208. *Nippon Steel Corporation and U.S. Steel Finalize Historic Partnership*, NIPPON STEEL (June 18, 2025), https://perma.cc/4SEW-FVAH; Stephen Heifetz, *The Nippon-U.S. Steel Deal, a Golden Share, and Magic Beans*, COUNCIL ON FOREIGN REL. (July 16, 2025), https://perma.cc/5WKG-YGYK.

Both examples of presidential involvement in economic transactions led some commentators to warn that these statutes enable a President to steer economic benefits toward allies.[209] Moreover, there is no requirement that the full terms of the deal be made public, and no built-in mechanism for congressional review of a qualified divestiture.[210] As questions are raised about the continued role of ByteDance and whether the sale met the intent of PAFACAA, Congress is in uncharted territory.[211] Even though Congress originated the law, there is limited role for congressional oversight. Finally, PAFACAA's granting the President the ability to require the sale of any "foreign adversary controlled application" opens the door for future Presidents to target any foreign-owned social media application.[212] This makes for an uncertain domestic investment environment, which could discourage foreign capital.[213]

e. Long Process Gave the Platform Time for a Public Relations Campaign

TikTok's popularity and the complicated process of finding a buyer allowed time for the platform to convince the American public that the platform should not be banned. TikTok launched an extensive advertising campaign aimed at persuading lawmakers and the American public of the need to retain the app and encouraged TikTok users to advocate to Congress on the app's behalf, which they did, passionately.[214] Some TikTok creators viewed the law as a threat to their

209. *See* John Cassidy, *Donald Trump's TikTok Deal Looks Like Crony Capitalism*, NEW YORKER (Sep. 29, 2025), https://perma.cc/M8X4-F289; Bobby Allyn & David Folkenflik, *Trump's TikTok Deal Payment Criticized as 'Shakedown Scheme' by Experts*, NPR (Sep. 26, 2025), https://perma.cc/Q9GT-KKDA. *TikTok USDS Announcement*, *supra* note 7, contains the public list of investors. *See also, e.g.*, Sam Kessler, Rebecca Ballhaus, Eliot Brown & Angus Berwick, *'Spy Sheikh' Bought Secret Stake in Trump Company*, WALL ST. J. (Jan. 31, 2026), https://perma.cc/8JZX-WPDV (regarding MGX's chairman); Bobby Allyn, *Who Is Larry Ellison, the Billionaire Trump Friend Who's Part of the TikTok Takeover?*, NPR (Oct. 6, 2025), https://perma.cc/AT6L-C5K6; Chase Peterson-Whithorn & Phoebe Liu, *The Web of Billionaire Pals, Partners and Trump Supporters Taking Control of TikTok*, FORBES (Sep. 25, 2025), https://perma.cc/KK6Y-7DC6. Since there was no direction in PAFACAA about how the deal should be negotiated, the involvement of the President's allies in the divestiture does not appear to conflict with PAFACAA.

210. *See* Conner, *supra* note 8; Short & Sobolik, *supra* note 168; 15 U.S.C. § 9901 note § 2(g)(6).

211. Representative John Moolenaar, Chairman of the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party, questioned whether the deal successfully removed China's influence over the algorithm and platform, and pledged "oversight," but it is unclear what form this oversight will take. Moolenaar, *supra* note 8.

212. 15 U.S.C. § 9901 note § 2(g)(3)(B).

213. Alexandra Alper & Steven Holland, *Golden Share in U.S. Steel Could Scare off Foreign Investors in US Deals, Lawyers Say*, REUTERS (June 16, 2025), https://perma.cc/8N7V-P8Q5; Isabella Wilkinson & Rowan Wilkinson, *The TikTok Transfer Raises Worrying Questions for Allies Like the UK*, CHATHAM HOUSE (Oct. 3, 2025), https://perma.cc/KGK7-4GVY. For a discussion of policy uncertainty impacting investment decisions, *see generally* Huseyin Gulen & Mihai Ion, *Policy Uncertainty and Corporate Investment*, 29 REV. FINANCIAL STUD. 523 (2016).

214. After PAFACAA passed, TikTok users wrote and called Congress to protest, urged on by the platform. Rebecca Kern, *Angry TikTok Users Are Still Flooding Congress with Calls*, POLITICO (Mar. 11, 2024), https://perma.cc/9V7K-8XQE. In 2025, TikTok's ad campaign was aimed at the public as well as lawmakers in the D.C. area. TikTok spent over $4.5 million on advertising between January and April 2025. Brian Schwartz, *TikTok Doubles Ad Buy to Fight Potential U.S. Ban as Congress Moves to*

livelihoods.[215] The intensity of the domestic opposition to closing TikTok would have further increased the difficulty of shutting down the app if no buyer had been found. By contrast, a rip-the-Band-Aid-off style ban may not leave time for this reaction. On the other side of the spectrum, comprehensive privacy regulation may not lend itself to a narrative of targeting.

f. The Whack-a-Mole Problem

The notion that ad hoc or one-off restrictions are an ineffective means of addressing underlying concerns is often repeated. The Internet Society noted that a TikTok divestiture is like "playing an expensive, dangerous game of 'whack-a-mole.'"[216] They argue that government restrictions on specific apps or online services fragment the global internet, destabilize user security, undermine economies, harm digital rights, and reduce equitable access to essential resources; they urge governments to instead adopt transparent, multistakeholder approaches by establishing international rules and norms to mitigate cyber threats.[217]

The TikTok saga provides several examples of how solving one problem may create others. The January 2026 deal left avenues for ByteDance to influence content on, and gain data from, the U.S. version of TikTok. Critics point out that ByteDance owns a stake in TikTok USDS and owns the recommendation algorithm, which TikTok USDS only licenses.[218] Moreover, as discussed above, TikTok USDS's role in operating TikTok in the United States may prove to be more limited than a "divestiture" would imply. ByteDance is reported to retain control over many revenue-generating operations—including advertising—through ByteDance-owned entities, meaning that TikTok USDS may not have independent commercial incentives.[219] And TikTok USDS's updated U.S. terms of service and privacy policy broaden the information it can collect and use, such as precise location (if enabled), users' interactions with TikTok's AI tools, and

---

Fast-Track Legislation, CNBC (Apr. 18, 2025), https://perma.cc/UG7W-VLRT. *See also* Christine Mui, *TikTok Tries to Sway DC with Ad Blitz*, POLITICO (Mar. 17, 2025), https://perma.cc/JE6Y-PCC2; Sapna Maheshwari, *With a U.S. Ban Looming, TikTok Portrays Itself as a Force for Good*, N.Y. TIMES (Mar. 25, 2025), https://perma.cc/5QB6-PMRY. High spending to avoid bans is not new for TikTok. Reporting shows that TikTok spent $1.3 billion to avoid bans in Europe; this money was primarily dedicated to the construction of data centers to prove that data would be stored locally. Chris Stokel-Walker, *TikTok Is Spending $1.3 Billion to Dodge Bans in Europe*, WIRED (Sep. 11, 2023), https://perma.cc/SA48-8N52.

215. Cherie Brooke Luo, *For This Creator, U.S. TikTok Ban 'Would Be Devastating'*, FORBES (Jan. 14, 2025), https://perma.cc/G67M-G4W3.

216. Natalie Campbell & John Perrino, *The Global Impact of a US TikTok Ban*, INTERNET SOC'Y (Jan. 10, 2025), https://perma.cc/B46H-G83Z. *See also* Final Service Podcast, *supra* note 199, at 23:00 (discussing how when people "talk about TikTok" they are not "just talking about TikTok" and suggesting that bans on Chinese companies like Shein may be next).

217. *Specific App and Service Bans are Fragmenting the Internet*, INTERNET SOC'Y (July 13, 2023), https://perma.cc/957S-B57N.

218. Short & Sobolik, *supra* note 168; Alan Z. Rozenshtein, *Lessons Learned from the TikTok Saga*, LAWFARE (Nov. 4, 2025), https://perma.cc/REZ4-TQQ3.

219. *TikTok USDS Announcement*, *supra* note 7; Conner, *supra* note 8.

expanded data use for ad targeting beyond TikTok.[220] TikTok USDS may end up holding an even richer dataset about its users. Finally, since TikTok USDS will be interoperable with the version of TikTok still operated by ByteDance, data and content flow between the two seems inevitable.[221]

Nor did the deal keep TikTok entirely in the hands of Americans. While TikTok USDS described itself as "majority American owned," the investor consortium is not exclusively U.S.-based.[222] ByteDance retains a 19.9% stake, and the remainder of the consortium includes several foreign investors.[223] Although partial foreign ownership was not prohibited by PAFACAA and is not in and of itself evidence of foreign influence via the app, the significant foreign investor base conflicts with proponents' portrayal of PAFACAA as requiring "an American takeover of TikTok."[224] Additionally, as the Grindr and PatientsLikeMe examples show, company ownership is fluid—some of the current owners could sell their shares to companies more friendly to China.[225]

---

220. *New Privacy Policy, supra* note 165; Rogers, *supra* note 165; Lily Jamali, *TikTok US Venture to Collect Precise User Location Data*, BBC (Jan. 23, 2026), https://perma.cc/6CFG-9YNF. PAFACAA does not impose additional requirements on the new owners with regard to user privacy. *See* Nicol Turner Lee, *TikTok May not Be Chinese-Owned Anymore, but There Still Is a Privacy Problem*, BROOKINGS (Oct. 2, 2025), https://perma.cc/A296-BJPS.

221. *See* Justin Sherman, *China Could Still Run Wild on TikTok After Trump's New Deal*, BARRON'S (Sep. 17, 2025), https://perma.cc/T3DE-2C3U.

222. *TikTok USDS Announcement*, *supra* note 7.

223. *Id.* NJJ Capital is the "family office" of Xavier Niel, a French citizen. *Id.* MGX was founded by the Emirate of Abu Dhabi. *Everson*, *supra* note 7. According to reporting, it "was launched by Mubadala, Abu Dhabi's sovereign wealth fund, and G42, an artificial intelligence holding company." *Id.* It is chaired by Sheikh Tahnoon bin Zayed Al Nahyan, the Deputy Ruler of Abu Dhabi and the National Security Advisor of the United Arab Emirates ("UAE"). *Our Leadership*, MGX, https://perma.cc/92VT-TE3E (last visited Jan. 31, 2026); *see also* Kessler, Ballhaus, Brown & Berwick, *supra* note 209. Sheikh Tahnoon is also the chairman of G42's Board of Directors. *G42 Announces Investment by Silver Lake*, G42 (Apr. 14, 2021), https://perma.cc/8QCY-DT8A. Among other investments, G42 was previously the sole shareholder of an app called "ToTok," which was removed from distribution by Apple and Google in 2019 due to suspicion it was used by the UAE to eavesdrop on users. Jon Gambrell, *Co-creator Defends Suspected UAE Spying App Called ToTok*, AP (Jan. 20, 2020), https://perma.cc/C8LJ-Y8CH; Mark Mazzetti, Nicole Perlroth & Ronen Bergman, *It Seemed Like a Popular Chat App. It's Secretly a Spy Tool*, N.Y. TIMES (Dec. 22, 2019), https://perma.cc/P7J6-F7UN. Yuri Milner is a former CEO and cofounder of Mail.ru, although he left Mail.ru in 2012. Robin Wauters, *Billionaire Yuri Milner Steps Down as Chairman of Mail.ru Group, Replaced by CEO Dmitry Grishin*, NEXT WEB (Mar. 14, 2012), https://perma.cc/Q5YN-VLWN. Milner used to be a Russian citizen and reportedly raised money from Russian-controlled banks to invest in Facebook and Twitter. Jesse Drucker, *Kremlin Cash Behind Billionaire's Facebook and Twitter Investments*, N.Y. TIMES (Nov. 5, 2017), https://perma.cc/NR3U-UPPD. In 2022, however, he renounced his Russian citizenship, citing the war in Ukraine. John Hyatt, *Early Facebook Investor Yuri Milner Renounces Russian Citizenship*, FORBES (Oct. 11, 2022), https://perma.cc/5GUK-MLJ2. He currently holds Israeli citizenship and resides in the United States. *Id.*

224. *See*, *e.g.*, John Moolenaar, *Krishnamoorthi, Moolenaar on D.C. Circuit Court Decision to Uphold TikTok Divestment Bill*, H. SELECT COMM. ON STRATEGIC COMPETITION BETWEEN THE U.S. & THE CHINESE COMMUNIST PARTY (Dec. 6, 2024), https://perma.cc/KJ4M-CBRW.

225. Even if the ownership does not change, the owners who acquired TikTok as a result of this deal could still handle user data in unsafe ways. *See* Lee, *supra* note 207. Moreover, some users raised concerns that the new owners would moderate content according to their own views. Geoff Bennett, Ali Schmitz & Dan Sagalyn, *TikTok Users Say They Are Being Censored After Change to U.S. Ownership*, PBS (Jan. 27, 2026), https://perma.cc/SYD6-JSLA.

The sale mitigated one vector for Chinese influence, leaving many others. When TikTok users thought that TikTok would "go dark" in January 2025, some began using a different Chinese app called Xiaohongshu.[226] Some have argued that the real benefit of TikTok to China is generating sales of Chinese-made goods, and this will continue despite the sale.[227] TikTok aside, Americans still provide plenty of their personal data to Chinese companies through other apps and websites.[228]

g. Divestiture as Part of a Multidimensional Relationship

The fall 2025 stage of the TikTok saga, in which the forced sale of TikTok was explicitly part of larger trade negotiations with China, showed how divestiture requirements can be part of a multidimensional relationship (or multilevel game).[229] The requirement for China to sell TikTok was perceived as offensive rather than defensive; the 2020 iteration of the divestiture requirement was described in an editorial by Xinhua, China's official news agency, as a "brazen heist."[230] When PAFACAA negotiations took place in 2025, however, China used the opportunity to negotiate with the Trump Administration about other aspects of the trade relationship.[231] The TikTok deal allowed China to avert high tariffs while possibly also laying the groundwork for a more favorable U.S. treatment of China in a conflict with Taiwan.[232]

---

226. The name literally translates to "Little Red Book," evoking Communist leader Mao Zedong's book of quotes, but its founder claimed the connection was unintentional. Victor Tangermann, *Man Named Mao Who Started Chinese App Called "Little Red Book" Was Actually Inspired by Stanford University and Mitt Romney*, FUTURISM (Jan. 15, 2025), https://perma.cc/2PMM-FCHD. For more about Xiaohongshu and its possible security issues, see Zeyi Yang, *With a TikTok Ban Looming, Users Flee to Chinese App 'RedNote'*, WIRED (Jan. 13, 2025), https://perma.cc/AW95-72A7; Wing Kuang, *Who's Afraid of the Little Red Book*, CHINA STORY (Jan. 20, 2025), https://perma.cc/RHM9-H8PB; Mona Wang, Jeff Knockel & Irene Poetranto, *Network Security Issues in RedNote*, CITIZEN LAB (Feb. 12, 2025), https://perma.cc/CQZ2-LPUQ.

227. SEARCH ENGINE PODCAST, *A Dubai Chocolate Theory of the Internet*, at 19:45–40:00 (Search Engine, Aug. 22, 2025), https://perma.cc/K94D-AC3L. *See*, *e.g.*, *id.* at 21:30 ("If we can get everyone to make ads, then those ads can become culture.").

228. *See* Chelsea Bailey, *The Other Chinese Apps Taking the US and UK by Storm*, BBC (Apr. 2, 2023), https://perma.cc/CW3P-VTWL; NICHOLAS KAUFMAN, SHEIN, TEMU, AND CHINESE E-COMMERCE: DATA RISKS, SOURCING VIOLATIONS, AND TRADE LOOPHOLES 2, 5 (2023), https://perma.cc/Z5RJ-VZRP (discussing Chinese e-commerce apps Shein and Temu, their reliance on U.S. consumer data, and previous platform security issues).

229. Negotiations led to a deal that addressed many—but not all—of the priorities of the two countries. ByteDance agreed to sell most of its stake in TikTok, but the deal did not completely wrest control from China or guarantee consumer privacy. See *supra* note 17 for a discussion of multilevel games, which is one way to view the fall 2025 trade negotiations with China.

230. Xinhua, *The TikTok Deal, a Brazen Heist*, CHINADAILY (Sep. 25, 2020), https://perma.cc/5U2W-RM6S ("By repeatedly using state power to suppress the private company without any proper justification, despite widespread protests from numerous TikTok users and concerns from industry observers, Washington has laid bare its true intention: to pull off a daylight heist."). Offensive and defensive actions are further discussed in notes 13 and 81 *supra*.

231. Lily Kuo, *Why China's Leader Xi Is Willing to Yield on TikTok*, N.Y. TIMES (Sep. 19, 2025), https://perma.cc/RS5D-Y94U.

232. One reporter observed, "For China, yielding on TikTok would be a way to offer the American president a symbolic win on an issue close to his heart — saving the hugely popular video app that he credits for helping him connect with young voters and win re-election. In exchange, Beijing would seek more room to negotiate on the matters it cares about most: tariffs, technology and Taiwan." *Id.*

During trade talks in October 2025, China negotiated a one-year suspension of the heightened "reciprocal" tariffs imposed by the Trump Administration (reducing the rate to 10% from 34%), and the United States agreed to a one-year relaxation of U.S. export controls for certain Chinese firms; these and other topics were discussed alongside TikTok.[233]

The reciprocal impact of PAFACAA across other countries remains an open question. The United States was one of the pioneers in forced divestiture of social media companies, with executive branch efforts coming into full swing in 2020 as CFIUS pursued Grindr and TikTok; other countries and U.S. states followed.[234] Observers note that the U.S. action may embolden other nations to assert similar control over foreign tech in their markets. For example, U.K. politicians have called for a ban or restrictions on TikTok following the U.S. law.[235] Authoritarian governments might also invoke the U.S. example to justify more sweeping bans on foreign platforms than they already have (for example, Russia could use it to justify tightening control over U.S.-based social networks, or China could retroactively justify its preexisting exclusion of Western apps under the pretext of reciprocity). Before PAFACAA came into effect, some experts postulated that it would draw reactive countermeasures from China.[236] This is still possible, even as China allows ByteDance to agree to a minority stake in TikTok USDS. As of January 2026, no international measures can be categorized as direct reactions to the new law; this may change as the effects of PAFACAA play out over the coming years.

C. Regulation Through a Comprehensive Data Privacy Law

This section discusses comprehensive data privacy regulations, which limit the collection of sensitive user data and its transfer to other jurisdictions. These laws provide broad standards of general application. These standards may prevent data

233. Trevor Hunnicutt, *Trump Shaves China Tariffs in Deal with Xi on Fentanyl, Rare Earths*, REUTERS (Oct. 30, 2025), https://perma.cc/E9L3-UQSZ; Donia Chiacu & Alexandra Alper, *US Delays Expansion of Export Restrictions on Chinese Firms After Trump-Xi Meeting, Bessent Says*, REUTERS (Oct. 30, 2025), https://perma.cc/D23B-D8XW; Michael Lowell, Philippe Heeren, Justin Angotti, Lizbeth Rodriguez-Johnson, Kristen Lowell & Erika Yeager, *Trump 2.0 Tariff Tracker*, REED SMITH (Nov. 20, 2025), https://perma.cc/F2CX-4LR2; *Fact Sheet: President Donald J. Trump Strikes Deal on Economic and Trade Relations with China*, WHITE HOUSE (Nov. 1, 2025), https://perma.cc/EA3G-YWQ3.

234. Final Service Podcast, *supra* note 199, at 23:00 (also discussing likely retaliation from China).

235. Vincent Manancourt, *Pressure on UK to Follow US in Toughening Stance on TikTok*, POLITICO (Mar. 18, 2024), https://perma.cc/BD87-FLAC (noting that former Conservative leader Iain Smith stated, "We should follow America. We should have done it ourselves. I've called for a ban before.").

236. *See, e.g.*, Xing Jiaying & Li Mingjiang, *The Potential Chinese Responses to a U.S. Ban on TikTok*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Apr. 11, 2024), https://perma.cc/79DM-JCLL ("Through a series of policy changes and public statements, Beijing has signalled that it won't be a passive actor in the TikTok settlement in the U.S. Rather than endorse the company's sale to mitigate ByteDance's commercial losses, Beijing is more likely to make a political decision to prohibit such a transaction under the guise of export control regulations. The approach could fuel sustained political discourse against Washington, fostering further diplomatic tension between China and the United States. ").

from being available for government surveillance and may be enforced against emerging threats. However, such broad regulations may be difficult to enact and have implications beyond countering surveillance. This section examines the EU's GDPR as an example of such a regulation and discusses efforts to pass similar responses in other countries. The GDPR is used as an example because it is arguably the world's most influential privacy law.

1. Overview of the GDPR

The GDPR, a law enacted by the EU,[237] was motivated by privacy threats arising from many corners, including State surveillance.[238] It applies not only to businesses in the EU but also to any entity, anywhere, that collects or targets the personal data of people in the EU.[239] Europe has a long history of valuing privacy. The right to privacy was included in the 1950 European Convention on Human Rights, and in 1995, the EU passed the Data Protection Directive.[240] This set minimum standards for privacy and security, which each EU country then referenced to create its own national laws.

The GDPR replaced this earlier Directive. It was passed by the European Parliament in 2016 and became fully enforceable on May 25, 2018.[241] The penalties for breaking the GDPR are severe. There are two levels of fines. The highest is up to €20 million or 4% of a company's global annual revenue, whichever is greater.[242] Additionally, individuals who claim that their data was mishandled have a right to seek compensation.[243]

Under the GDPR, "personal data" includes any information that can be linked to a specific person. This often includes names, email addresses, location data,

237. GDPR, *supra* note 9.

238. These include threats to privacy from commercial, criminal, and governmental actors, as well as a recognition of a "right to be forgotten." *Id.* recital 75. Recital 75 lists many risks to the "rights and freedoms of natural persons" which the GDPR protects. This includes the risks that typically arise from criminal activity, such as identity theft, fraud, financial loss, and loss of confidentiality of professional information, and damage to reputation, as well as risks that may arise from commercial entities including personal profiling (e.g., based on health data), prediction of work performance, and discrimination. *Id.* Recital 75 also lists risks that are often associated with government surveillance, such as compilation of political opinions, religion, genetic and location information. *Id.* For a discussion of the purpose limitation of Article 5(1)(b) as rooted in the European Charter but limiting "big data" processing by commercial and government actors, *see* Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1005–06 (2017). For an analysis of the right to be forgotten (codified in Article 17) as a driver of the GDPR, see Alessandro Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'*, 29 COMPUTER L. & SEC. REV. 229 (2013). For a discussion of U.S. surveillance and the Snowden leaks as motivating the GDPR, see Coyne, *supra* note 47. *See also* Augustín Rossi, *How the Snowden Revelations Saved the EU General Data Protection Regulation*, 53 INT'L SPECTATOR 95 (2018).

239. GDPR, *supra* note 9, art. 3(2).

240. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC) (repealed 2018), https://perma.cc/C4TJ-WSG4.

241. GDPR, *supra* note 9, art. 99(2).

242. *Id.* art. 83(5).

243. *Id.* art. 82(1).

race, gender, fingerprints, religion, web tracking cookies, and political beliefs.[244] Even pseudonymized data may be "personal" if it can be linked to a real person. "Data processing" includes doing anything with personal data, including collecting, storing, using, or deleting it.[245] Companies that handle personal data must follow seven key principles: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.[246]

Companies, i.e., any controllers or processors within the territorial scope, whether or not incorporated in the EU, must be able to prove compliance with GDPR rules; this may include assigning staff to handle data protection and appointing a Data Protection Officer.[247] Companies must keep data safe using technical tools such as encryption and two-factor authentication, as well as organizational policies.[248] There are rules governing the reporting of data breaches. Systems and processes must incorporate data protection by design.[249] There are enumerated reasons for when companies may process data, such as when the subject gives consent (which must be clear, specific, and voluntary)[250] or collection is legally required.[251] Under the GDPR, individuals have rights to their personal data including the rights to be told what data gets collected (to be informed), to see their data (access), to fix incorrect data (rectification), to have data deleted (erasure), to limit how data is used (restrict processing), to move their data to another provider (portability), to say no to data use (object), and not to be subject to automated decisions or profiling.[252]

2. GDPR as Applied to Social Media Surveillance

Under EU law, personal data may not be exported to countries lacking "essentially equivalent" privacy protections.[253] The GDPR allows data transfers to third countries through several mechanisms.[254] A data transfer may proceed based on an adequacy decision by the European Commission, determining that a country or transfer framework offers equivalent protections.[255] Without an adequacy decision, a transfer can only occur if there are "appropriate safeguards" in place.[256] These could include corporate rules, standard contractual clauses (set language approved by the European Commission), and codes of conduct that carry

244. *Id*. art. 4(1).
245. *Id*. art. 4(2).
246. *Id*. art. 5(1).
247. *Id*. recital 77.
248. *See id*. recital 78, 83.
249. *Id*. art. 25(1).
250. *Id*. art. 6(1)(a), 7(2).
251. *Id*. art. 6(1)(c).
252. *Id*. art. 12–23.
253. *Id*.; *International Data Transfers*, EUR. DATA PROT. BD.: DATA PROT. GUIDE FOR SMALL BUS., https://perma.cc/5HEJ-F2UX.
254. GDPR, *supra* note 9, art. 44–50, recitals 101–116.
255. *Id*. recitals 103–06.
256. Id. art. 46.

enforceable commitments.[257] Individual data controllers may also receive certification.[258] If neither an adequacy decision nor safeguards exist, transfers can occur based on an exemption, such as a data subject's explicit, informed consent.[259]

In a transatlantic legal battle beginning around 2013, Austrian privacy advocate Max Schrems argued that Facebook Ireland's transfer of EU citizens' data to the United States was not compliant with EU privacy laws.[260] In *Schrems I*—which predated the GDPR—the Court of Justice of the EU ("CJEU") invalidated the *EU-U.S. Safe Harbor* agreement of 2000, which had allowed companies to transfer EU data to the United States. Relying in part on Edward Snowden's revelations about U.S. use of information collected under FISA Section 702, the CJEU found that U.S. law violated EU citizens' fundamental rights by failing to protect their data from indiscriminate intelligence access.[261] In an attempt to comply with the CJEU ruling and assuage European concerns, the EU and the United States negotiated a replacement framework (*Privacy Shield*) in 2016, which required participating U.S. companies to self-certify compliance with privacy principles.[262] In 2020, after the GDPR came into effect, the CJEU struck down the *Privacy Shield* in *Schrems II*, a second decision, again citing U.S. FISA surveillance and the absence of equivalent privacy rights for non-Americans, this time applying the GDPR.[263] On July 10, 2023, the European Commission adopted an adequacy decision for the new *EU-U.S. Data Privacy Framework* ("DPF"), concluding that the United States provides a level of data protection comparable to the EU for companies participating in the DPF.[264] Participation is opt-in: only U.S. companies that self-certify to the Department of Commerce and publicly

257. *Id.* art. 46, recitals 107–10.

258. *Id.* art. 42.

259. *Id.* recitals 107, 111.

260. Case C-362/14, Schrems v. Data Prot. Comm'r (*Schrems I*), ECLI:EU:C:2015:650, ¶ 1 (Oct. 6, 2015).

261. *Id.* ¶¶ 1, 21, 81, 98, 107.

262. *See* GDPR, *supra* note 9, art. 45; *Privacy Shield* was a data-transfer framework under which participating U.S. companies self-certified to Department of Commerce privacy principles, enforceable primarily by the Federal Trade Commission, that the European Commission treated as providing "adequate" protection for transfers of EU personal data. U.S. DEP'T OF COM., EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES 1 (2016), https://perma.cc/V25V-GNKM.

263. The CJEU found the U.S. treatment of European data incompatible with GDPR Article 45(1), which requires that a country receiving data from the EU ensure an "adequate level of protection" for the data, following factors listed in Article 45(2). Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. (*Schrems II*), ECLI:EU:C:2020:559, ¶ 199 (July 16, 2020). The *Privacy Shield* agreement, which did not limit U.S. agencies' ability to access data under FISA, was insufficient to guarantee an adequate level of protection. *Id.* The CJEU explained, "It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes." *Id.* ¶ 180. *See* GDPR, *supra* note 9, arts. 45, 99.

264. Commission Implementing Decision EU 2023/1795 of 10 July 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–U.S. Data Privacy Framework, 2023 O.J. (L 231) 1 [hereinafter Adequacy Decision]; U.S. DEP'T OF COM., EU-U.S. DATA PRIVACY FRAMEWORK PRINCIPLES (2023), https://perma.cc/B8W2-CT9B [hereinafter DPF].

commit to the DPF Principles are covered by the adequacy decision for their EU-U.S. transfers.[265] The participant list includes major social media firms (e.g., Meta Platforms, Inc.).[266] This came after the United States adopted EO 14086, "Enhancing Safeguards for United States Signals Intelligence Activities," which created a mechanism for EU citizens and some others to submit complaints about misuse of their data by the U.S. Intelligence Community.[267]

Facebook is not the only social media platform that the GDPR has been used to address. In May 2025, Ireland's Data Protection Commission ("DPC") fined TikTok €530 million for violating the EU's GDPR by transferring European user data to China without ensuring adequate protection.[268] The DPC found that TikTok initially failed to disclose that European user data was stored on servers in China.[269] TikTok further failed to demonstrate that when European data was accessed by staff in China, that data was afforded EU-equivalent privacy guarantees.[270] TikTok's assessment presented to the Data Protection Commission did not account for potential access by Chinese authorities under China's national security laws.[271] The DPC ordered TikTok to bring its data processing practices into compliance within six months or face suspension of data transfers to China.[272] TikTok has announced plans to appeal the decision, arguing that the ruling does not reflect current safeguards, including its €12 billion Project Clover

265. DPF, *supra* note 264, §§ I.3, III.6.

266. *Meta Platforms, Inc.*, DATA PRIVACY FRAMEWORK PROGRAM, https://perma.cc/KYQ2-QAZJ (last visited Jan. 2, 2026).

267. EO 14086, *supra* note 50. Citizens of designated countries can submit complaints to the Civil Liberties Protection Officer (CLPO) within ODNI, via an office designated by their home government (called a "public authority"). *Id.* § 3(c). The CLPO must review the complaint, determine if a violation of U.S. law was committed that adversely affects the complainant's privacy interests, identify remediation if so, and issue a response to the complainant stating whether a violation was identified. *Id.* §§ 3(c)(i), 4(d). The decisions of the CLPO can be appealed to the Data Protection Review Court. *Id.* § 3(d)(B). The complaint must allege a violation and must provide the information forming the basis of the belief that the violation occurred. *Id.* § 3(k). The EO does not require the complainant to demonstrate that their data has actually been subject to U.S. intelligence activities. *Id.* § 3(k)(ii). While this raises the question of how someone could suspect that they were subject to improper intelligence activities, an individual could submit a complaint based on circumstantial evidence (for example, if they were able to tell personal data had been compromised and inferred U.S. intelligence agencies played a role). The CLPO would review these allegations. Currently designated countries include the EU, United Kingdom, Switzerland, Norway, Iceland, and Liechtenstein. *What Is a "Qualifying State?", Data Protection Review Court Frequently Asked Questions*, OFF. OF PRIV. & C.L., U.S. DEP'T OF JUST. (Sep. 16, 2024), https://perma.cc/44V7-8VCP.

268. *Irish Data Protection Commission Fines TikTok €530 Million and Orders Corrective Measures Following Inquiry into Transfers of EEA User Data to China*, IR. DATA PROT. COMM'N (May 2, 2025) [hereinafter *Irish Data Commission Press Release*], https://perma.cc/V6SD-XFSD (In this press release, the Data Protection Commission stated they "will publish the full decision and further related information in due course."); Ryan Browne, *Ireland Fines TikTok 530 Million Euros for Sending EU User Data to China*, CNBC (May 2, 2025), https://perma.cc/2PL3-95MP.

269. *Irish Data Commission Press Release*, *supra* note 268.

270. *Id.*

271. *Id.*

272. *Id.*

data security initiative,[273] and asserting that it has never provided European user data to Chinese authorities.[274]

Other EU laws have recently begun to regulate other aspects of social media platforms. The Digital Services Act (DSA), passed in 2022, requires "very large online platforms" (a term that includes popular social media companies) to identify and mitigate certain risks arising from the speech on their platforms.[275] Risks include "any actual or foreseeable negative effects on civic discourse and electoral processes, and public security" as well as "gender-based violence" and "the protection of public health."[276] While the GDPR addresses social media surveillance, the DSA attempts to mitigate social media manipulation. The risks noted in the DSA are similar to the surveillance concerns motivating PAFACAA, addressed in Sections III.B.1.a *supra* and IV.A.3 *infra*. In December 2025, the European Commission fined X €120 million for breaching its DSA obligations, including by deceptive design of the blue "verified" checkmark (since it indicates authenticity but can really be purchased by any user).[277]

3. GDPR-Like Efforts in Other Countries

In the second half of 2024, several countries—such as Cameroon, Ethiopia, Malawi, Moldova, and Vatican City—enacted new data privacy laws, while others, including Malaysia, introduced amendments to align more closely with international standards like the EU's GDPR.[278] They joined a host of other countries that had previously been inspired by the GDPR, including Brazil, which adopted the Lei Geral de Proteção de Dados in 2020—the nation's first comprehensive data protection law.[279]

---

273. TikTok's "Project Clover" is a ten-year European data-security program, echoing "Project Texas," *supra* note 193. European users' data will be kept in a "European data enclave" in regional data centers (Ireland and Norway, with a new site planned in Finland). NCC Group, a U.K.-based cybersecurity firm, will independently monitor data access. *Project Clover: €1 Billion Investment in Finland for New Data Center*, TIKTOK (May 6, 2025), https://perma.cc/W4VN-E6XZ.

274. Browne, *supra* note 268.

275. DSA, *supra* note 9, arts. 34–35.

276. *Id.* art. 34(1)(c)-(d).

277. *Commission Fines X €120 Million under the Digital Services Act*, EUR. COMM'N (Dec. 4, 2025), https://perma.cc/BM5S-FK7J.

278. Countries' changes included stricter breach notification timelines, expanded cross-border data transfer rules, and requirements to appoint data protection officers. As of late 2024, 144 countries—representing approximately 6.64 billion people, or 82% of the global population—have enacted national data privacy laws, up from 79% the previous year. Africa and Asia have shown progress, with over 70% of countries in each continent now having comprehensive laws. Some of the world's most populous countries—including the United States, Pakistan, Bangladesh, Iran, and Iraq—still lack a comprehensive national privacy law. Aly Apacible-Bernardo & Kayla Bushey, *Data Protection and Privacy Laws Now in Effect in 144 Countries*, INT'L ASSN. OF PRIV. PROS. (Jan. 28, 2025), https://perma.cc/A855-KF6L.

279. John J. Isaza & Hannah Katshir, *Brazil Passes Landmark Privacy Law: The General Law for the Protection of Privacy*, BUS. L. TODAY (Apr. 24, 2020), https://perma.cc/RY57-96G9 ("Joining the global trend originating in Europe with the General Data Protection Regulation (GDPR), Brazil recently enacted its own omnibus law governing the use of personal data, the Lei Geral de Proteção de Dados (LGPD), or General Law for the Protection of Privacy.").

Federal privacy legislation in the United States gained renewed momentum in 2019 after the enactment of the EU's GDPR. Senator Ed Markey's Privacy Bill of Rights Act emphasized opt-in consent.[280] Senator Maria Cantwell introduced the Consumer Online Privacy Rights Act,[281] while Senators Roger Wicker and Marsha Blackburn introduced the SAFE DATA Act.[282] These efforts ultimately stalled due to a lack of consensus and the onset of the COVID-19 ("Covid") pandemic.

In 2022, as U.S. states continued to enact their own privacy laws, Representative Frank Pallone introduced the American Data Privacy and Protection Act ("ADPPA").[283] ADPPA seemed to have momentum.[284] It called for a comprehensive federal data privacy law that applied uniformly to all companies, foreign and domestic, rather than targeting specific apps.[285] It would require entities to disclose the types of data they collect, how the data is used, how long the data is retained, and whether the data is made accessible to China and other countries.[286] Despite clearing the House Energy & Commerce Committee in July 2022, the ADPPA never received a House floor vote and expired at the end of the 117th Congress; Speaker Nancy Pelosi and California officials opposed its state-law preemption approach, among other issues.[287] In summer 2024, the "American Privacy Rights Act" ("APRA") was introduced, representing one of the latest proposals for comprehensive data privacy legislation.[288] APRA's key innovation is to grant consumers data privacy rights regarding their data held by covered entities, including rights of access, correction, deletion, and portability.[289] APRA would impose data minimization requirements and transparency duties, and would allow consumers to opt out of targeted advertising and certain data transfers.[290] APRA would enable enforcement by the Federal Trade Commission and state attorneys general (with a private right of action) and preempt most state comprehensive privacy laws.[291]

280. Privacy Bill of Rights Act, S. 1214, 116th Cong. (2019).

281. Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019).

282. SAFE DATA Act, S. 2499, 117th Cong. (2021).

283. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

284. JONATHAN M. GAFFNEY, ERIC N. HOLMES & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB 10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 4–5 (2022).

285. *Id.* at 1.

286. *Id.* at 2.

287. *See Pelosi Rejects Bipartisan Privacy Bill*, AXIOS (Sep. 1, 2022), https://perma.cc/K5KD-8KYX; H.R. 8818, 118th Cong. (2024).

288. *See* American Privacy Rights Act, H.R. 8818, 118th Cong. (2024).

289. *Id.* § 105.

290. *Id.* §§ 102, 104, 106.

291. *Id.* §§ 115, 116. *See also* CHRIS D. LINEBAUGH, PETER J. BENSON, JONATHAN M. GAFFNEY, MATTHEW D. TROUT & CLAY WILD, CONG. RSCH. SERV., LSB11161, THE AMERICAN PRIVACY RIGHTS ACT (2024)*; The American Privacy Rights Act of 2024 Explained: What Does the Proposed Legislation Say and What Will It Do?*, TECH POLICY (Apr. 18, 2024), https://perma.cc/DEA8-XRL5.

4. Lessons from this Approach

A comprehensive data privacy law approach is adaptable. The challenges to Meta and TikTok under GDPR, discussed in Section III.C.2 *supra*, show how a platform-agnostic rule can still reach specific firms. Moreover, comprehensive regulation is more consistent with the principles of free speech and fairness. Legislators can establish uniform standards and some level of built-in due process for regulatory decisions, in contrast to frequently unreviewable or opaque executive branch decision-making. Comprehensive regulation can also take a principled approach to protect consumer privacy. For example, while PAFACAA is only concerned with removing "adversary" control of Americans' data, the GDPR is concerned with protecting internet users' data from any privacy violations.

Respecting these principles comes with the additional benefit that the regulation is less likely to be perceived by an adversary as "offensive" or escalatory since it is platform-neutral and more likely to be understood as defensive.[292] Framing regulation in terms of protecting privacy may make it easier to explain and justify to the public. In other words, neutrality and process discipline communicate that the State is constraining how everyone handles data, not targeting the owners of a specific platform, reducing escalation incentives while still addressing the underlying security risk. The more permanent, less ad hoc nature of comprehensive regulation means that affected countries are likely to treat the regulation as a fact on the ground rather than negotiate or retaliate their way out of the regulation; the U.S. reaction to the GDPR (attempting to comply) may be an example of this. This does not completely rule out the danger that an action carried out by an EU State to enforce the GDPR could be seen as offensive, but the GDPR provides a ready explanation and set of testable rules.

Another lesson is that the standards this approach introduces tend to spread, whether through compliance in other jurisdictions with the enacted laws or copycat regulation. People in other countries see some of the benefits. The enactment of the GDPR in 2018 has had a so-called "Brussels Effect" on data privacy norms beyond Europe's borders.[293] As one of the strictest data protection laws, the GDPR imposed comprehensive requirements on any organization handling EU residents' personal data, regardless of where the organization is located. This extraterritorial reach effectively exported EU privacy standards worldwide. In its wake, numerous countries introduced GDPR-inspired laws, as discussed above. Even jurisdictions with preexisting frameworks—such as Singapore, New Zealand, and Switzerland—amended their laws to more closely mirror GDPR-era standards.[294] This global wave of GDPR mirroring has been motivated in part by a desire to facilitate international data flows. Given the global nature of the modern

292. Offensive and defensive actions are further discussed in notes 13 and 81 *supra*; the security dilemma is discussed in notes 14 and 82 *supra*.

293. Anu Bradford, *The Brussels Effect*, 107 NORTHWESTERN U. L. REV. 1, 3 (2012) (arguing that the EU has the powerful ability to promulgate regulations that influence other countries' legal frameworks).

294. Apacible-Bernardo & Bushey, *supra* note 278.

economy, countries seek "adequacy" status under EU law to avoid being shut out of EU data transfers. Roughly 144 countries now have some form of data privacy laws, covering over 6.6 billion people—exceeding 80% of the world's population.[295] This is an example of players successfully cooperating in an assurance game, with the caveat that future success depends on continued adoption and enforcement of these laws.

Calls in the United States to reform FISA Section 702 to appease European privacy demands illustrate how foreign pressure can drive changes to U.S. national law.[296] Major U.S.-based tech companies have had to substantially adjust their practices globally to comply with EU rules, from overhauling privacy policies to offering EU-style data rights to users worldwide.[297] Companies like Facebook (Meta) and Google faced hefty fines (up to billions of dollars) under the GDPR's enforcement mechanism, signaling the EU's willingness to come down hard on foreign firms.[298] This dynamic occasionally causes friction: European regulators assert jurisdiction over U.S. companies in the name of privacy, while U.S. industry and officials sometimes view the GDPR as a trade barrier or foreign regulation of American businesses.[299] Although bipartisan support for PAFACAA was justified in part by concerns that "foreign adversary controlled applications" could be used to push misinformation, disinformation, and propaganda, the DSA has drawn criticism from the Trump Administration for perceived overreach.[300] In December 2025, after the European Commission announced its fine of X, Secretary of State Marco Rubio announced visa and entry bans targeting five Europeans who drafted or advocated for the DSA (including former EU Commissioner Thierry Breton), accusing them of coercing platforms into censoring American viewpoints and imposing burdensome regulation under the DSA.[301] This is an example of how one jurisdiction's cross-cutting regulatory posture can elicit

295. *Id.*

296. *See* CHRIS D. LINEBAUGH & EDWARD C. LIU, CONG. RSCH. SERV., R46724, EU DATA TRANSFER REQUIREMENTS AND U.S. INTELLIGENCE LAWS: UNDERSTANDING SCHREMS II AND ITS IMPACT ON THE EU-U.S. PRIVACY SHIELD (2021). This can be seen as a defensive action (GDPR) effectively limiting a U.S. proactive collection (arguably an "offensive" action) by inducing a change in U.S. policy.

297. *EU Digital Regulations Are Costing U.S. Tech Firms Billions Annually*, COMPUT. & COMMC'N INDUS. ASS'N (Mar. 11, 2025), https://perma.cc/5BWR-24P5.

298. Adam Satariano, *Meta Fined $1.3 Billion for Violating E.U. Data Privacy Rules*, N.Y. TIMES (May 22, 2023), https://perma.cc/JVM9-ENCR; Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (June 21, 2019), https://perma.cc/3ND8-W532.

299. *See*, *e.g.*, J.D. Vance, *Remarks by the Vice President at the Artificial Intelligence Action Summit in Paris, France*, AM. PRESIDENCY PROJECT (Feb. 11, 2025), https://perma.cc/6V8V-SSX6 ("[F]or smaller firms, navigating the GDPR means paying endless legal compliance costs or otherwise risking massive fines.").

300. *Id.* ("Many of our most productive tech companies are forced to deal with the EU's Digital Services Act and the massive regulations it created about taking down content and policing so-called misinformation.").

301. Marco Rubio, *Announcement of Actions to Combat the Global Censorship-Industrial Complex*, U.S. DEP'T OF STATE (Dec. 23, 2025), https://perma.cc/JQC8-TQEA. Sudip Kar-Gupta & Charlotte Van Campenhout, *Europe Slams Visa Bans After U.S. Takes Fresh Swing at Allies Over "Censorship"*, REUTERS (Dec. 24, 2025), https://perma.cc/K8Y8-5JW2; Steven Lee Myers, *U.S. Bars 5 European Tech Regulators and Researchers*, N.Y. TIMES (Dec. 23, 2025), https://perma.cc/935A-MSJC.

retaliatory measures from another jurisdiction. At the same time, many U.S. states have followed the global trend—California's Consumer Privacy Act (2018), for example, grants rights of access and deletion similar to the GDPR.[302]

This reciprocal legal borrowing underscores that data privacy has evolved into a transnational regulatory conversation. A country's privacy regime now directly impacts others, both by inspiring legislation and by altering how cross-border data is handled in practice. If the EU had just required a divestment of Facebook in the EU, or an outright ban, positive dialogue might not have resulted. Instead, the GDPR's enactment and subsequent transatlantic negotiations led to the development and recognition of privacy interests and redress rights for non-USPs, as discussed above, culminating in the Data Protection Review Court mechanism established under EO 14086 in 2022.[303] This was a concession to address the CJEU's concerns about FISA surveillance. Whether these changes suffice is pending further review (often dubbed a potential "Schrems III").

There are challenges to this approach. Enacting such a law in many countries would be politically difficult, as seen in the United States. Broad personal privacy protections could conflict with domestic intelligence interests or impose costly compliance burdens on businesses.[304] Moreover, enforcing any new regulation through litigation and regulatory findings may be slow and uncertain. Constitutional concerns are not limited to ban or divestiture approaches. For example, as Justice Gorsuch noted in his concurring opinion in *TikTok Inc. v. Garland*, any new compliance regime might raise serious issues if it requires the government to monitor Americans' data flows to ensure they are not being transferred abroad[305]—and depending on how a comprehensive law is written, it could trigger this concern.

At a higher level, the GDPR presents a case study in how countries react to each other's surveillance laws. One nation's security regime (the United States')

302. California's Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE § 1798.100 et seq.

303. For an overview of how complaints may be processed under EO 14086, see *supra* note 267. By providing a way to challenge U.S. intelligence agencies' handling of EU citizens' data, EO 14086 enables an "adequate level of protection" under GDPR art. 45 and meets the "effective remedy" requirement of art. 47 of the EU Charter of Fundamental Rights. *See* GDPR, *supra* note 9; Charter of Fundamental Rights of the European Union art. 45, 2012 O.J. (C 326) 391, 404. This enabled the European Commission's 2023 adequacy decision upholding the EU-U.S. Data Privacy Framework. Adequacy Decision, *supra* note 264.

304. The United States and other countries considering comprehensive privacy legislation must play a multi-level game, taking into account domestic politics, national security and intelligence needs, and relationships with/responsibilities to the international community. *See* Putnam, *supra* note 17.

305. TikTok Inc. v. Garland, 604 U.S. 56, 84–85 (2025) (Gorsuch, J., concurring in the judgment) ("[A]ny new compliance regime could raise separate constitutional concerns—for instance, by requiring the government to surveil Americans' data to ensure that it isn't illicitly flowing overseas."). While Justice Gorsuch did not specify which constitutional provisions might be violated, warrantless government surveillance of Americans' communications could possibly raise Fourth Amendment concerns if considered an unreasonable search, or First Amendment concerns if the surveillance chills speech. *See also Leading Case: TikTok Inc. v. Garland*, 139 HARV. L. REV. 280, 288 (2025) ("Justice Gorsuch acknowledged that the Court's TikTok holding may contradict 'the wisdom of Justice Brandeis in *Whitney* and Justice Holmes in *Abrams*,' opinions that respectively form the urtexts of two leading strands of First Amendment theory.") (internal citations omitted).

prompted a legal backlash in another political organization (the EU). As discussed above, in the aftermath of the 2013 Snowden revelations about U.S. intelligence programs, European authorities grew alarmed. These revelations—outlined in Section II.A—demonstrated how FISA-authorized surveillance allowed U.S. agencies to collect vast amounts of data from foreign users via social media platforms. This prompted individual litigation (*Schrems I* and *II*), regulatory reform in the EU (GDPR), and a reworking of the U.S.-EU data privacy framework. In this case, individual litigation, enabled by regulatory reform and enforced by the EU courts, led to the renegotiation of a framework affecting the whole EU.

There is a growing interdependence of national data governance regimes. The interplay of FISA, the GDPR, *Schrems*, the Great Firewall, China's surveillance laws, and PAFACAA (to name just a few legal developments) demonstrates that privacy regulation is a multi-way street. Understanding these reciprocal influences helps lawyers and policymakers make sense of the traffic as countries double down on unilateral measures. Digital protectionism and escalating measures may lead to a fractured global internet increasingly defined by *ad hoc* solutions to surveillance.

IV. ANOTHER OPTION: DEVELOPMENT OF INTERNATIONAL RULES AND GUIDELINES

As seen in the previous sections, unilateral responses such as bans, divestment, and privacy regulation can only get States so far. None of the unilateral approaches, even comprehensive privacy regulations, address all possible social media threats, or address threats against the international community. Moreover, States have increasingly engaged in social media surveillance and manipulation,[306] including the use of AI,[307] even as State responses are implemented. This section proposes a fourth strategy that can complement unilateral action: the development of international rules and guidelines.

This section discusses two examples of international legal development: application of the rule against intervention to State actions over social media and increased reliance on the OECD Privacy Guidelines. The former involves evolution of binding customary international law ("CIL"), while the latter involves adoption of non-binding guidelines. Neither approach would prohibit intelligence gathering, but both approaches would represent international agreement on the

306. Sanja Kelly, Mai Truong, Adrian Shahbaz, Madeline Earp & Jessica White, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*, FREEDOM HOUSE (Nov. 2017), https://perma.cc/6KV6-CCQN; *see generally* SAMANTHA BRADSHAW, HANNAH BAILEY & PHILIP N. HOWARD, INDUSTRIALIZED DISINFORMATION: 2020 GLOBAL INVENTORY OF ORGANIZED SOCIAL MEDIA MANIPULATION (2021); Adrian Shahbaz & Allie Funk, *Social Media Surveillance*, FREEDOM HOUSE (Nov. 2019), https://perma.cc/EL7S-WADY. For a description of how companies have less capacity to protect platform integrity against commercial actors, see ROLF FREDHEIM, SEBASTIAN BAY, ANTON DEK, MARTHA STOLZE & TETIANA HAIDUCHYK, SOCIAL MEDIA MANIPULATION 2022/2023: ASSESSING THE ABILITY OF SOCIAL MEDIA COMPANIES TO COMBAT PLATFORM MANIPULATION (2023).

307. Jeremy Hsu, *US Government Is Using AI for Unprecedented Social Media Surveillance*, NEW SCIENTIST (May 5, 2025), https://perma.cc/RW9V-NM9K.

boundaries of acceptable conduct.[308] Both would result in more uniform global responses to State surveillance or manipulation. Both also require a high degree of coordination between States, since they depend on States adopting similar policies or norms of behavior for the potential reward of a safer online environment for everyone.[309]

A. Development of Customary International Law: The Rule Against Intervention

The development of CIL is one way in which coordination between States can discourage the most serious forms of social media interference. CIL develops through State practice, motivated by a sense of legal obligation (*opinio juris*).[310] Development of an area of CIL is slow and difficult—it poses a significant coordination problem, since international recognition of a rule requires consistent practice across States and acknowledgement that the practice is motivated by adherence to CIL.[311] Moreover, if a State persistently objects to a particular rule, that State is arguably not bound by it.[312] Once a CIL rule achieves widespread recognition, however, it influences behavior by setting baseline expectations.[313]

---

308. There is little precedent for an international rule against espionage *per se*. *See* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 293 (2015) ("Why has international law had so little to say about how, when, and where governments may spy on other states and foreign citizens, including by electronic means? Historically . . . states sensibly concluded that the benefits to unregulated spying were high and the corresponding costs were low.") The International Group of Experts behind the Tallinn Manual "agreed that there is no prohibition of espionage *per se*," even though an operation undertaken for espionage purposes could violate another international rule or norm. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 168–69 (Michael N. Schmitt ed., 2d ed. 2017). The Department of Defense Law of War Manual agrees that cyber operations "resemb[ling] traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information" are not forbidden and adds that the "United States conducts such activities via cyberspace." OFF. OF GEN. COUNS., U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 16.3.2 (June 12, 2015) (C4, July 31, 2023) [hereinafter DOD LAW OF WAR MANUAL]. Deeks argues that States may now be more willing to develop boundaries for espionage and proposes six norms as a "framework for surveillance," to include clear domestic rules, requiring reasons for data collection, periodic review, limits on retention, clear domestic rules, and neutral oversight bodies. Deeks at 327–28, 351–62. In sum, States are very unlikely to agree to rules that completely forbid foreign surveillance of traffic online, but they might accept narrower guardrails that preserve security interests. Governments may, of course, still violate agreed-upon rules in secret, but having agreed frameworks raises the diplomatic and reputational costs of doing so and makes violations easier to call out.

309. Development of international rules and norms can be viewed as a multiplayer, multilevel assurance game requiring coordination between many States. *See supra* notes 15 and 17.

310. ALLEN S. WEINER, DUNCAN B. HOLLIS & CHIMÈNE I. KEITNER, INTERNATIONAL LAW 136–42 (8th ed. 2023).

311. It is not required that all States follow the practice all the time, but that a practice be "general and consistent." RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 102 cmt. b (A.L.I. 1987) ("A practice can be general even if it is not universally followed; there is no precise formula to indicate how widespread a practice must be."). *See also* LOUIS HENKIN, HOW NATIONS BEHAVE: LAW AND FOREIGN POLICY 47 (2d ed. 1979) ("It is probably the case that almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time.").

312. WEINER, HOLLIS & KEITNER, *supra* note 310, at 148–50.

313. "The fact that particular behavior is required by law brings into play those ultimate advantages in law observance that suppress temptations and override the apparent immediate advantages from acting otherwise." HENKIN, *supra* note 311, at 98. For a discussion of the role of the International Court

These expectations can encourage reciprocal actions that reinforce a rule, rather than retaliation.[314]

1. How a Rule Against Intervention Could Change State Behavior

The rule against intervention is used in this article as an example of an area of CIL that could be developed to set minimum expectations for interference with another country's internal affairs over social media. The rule prohibits a State from coercively interfering in the sovereign affairs of another State.[315] As new technology provides new ways to intervene in sovereign affairs, government officials have discussed how this rule might apply to new forms of intervention. This section suggests that the rule could develop to prohibit the worst outcomes of State manipulation via social media; the rule would not prohibit intelligence gathering. While earlier sections of this article discussed the risks of States perceiving other States' actions as offensive, a rule against intervention can be seen as establishing a presumption that certain actions are offensive.[316] When a country is considering the costs of committing a prohibited intervention, it will know that its actions will be perceived as offensive by an affected country, changing the risk calculus.

International law matters, even if it is not followed all the time.[317] When domestic policies like PAFACAA can claim a foundation in international law, political disputes are informed by legal norms. These norms help legislatures,

---

of Justice in determining CIL, see Stefan Talmon, *Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion*, 26 EUR. J. INT'L L. 417 (2015).

314. In the language of international relations game theory, CIL can develop when "states face and solve bilateral *coordination* problems. If states coordinate on identical or symmetrical actions, they receive higher payoffs than if they do not coordinate." Jack L. Goldsmith & Eric A. Posner, *A Theory of Customary International Law*, 66 U. CHI. L. REV. 1113, 1115 (1999). CIL can also be developed through "true cooperation" during which states enjoy long-term cooperation toward mutual goals. *Id.* Goldsmith and Posner identify, however, that much of the time, CIL develops through coincidence of interest (a uniform practice develops because it is beneficial to both states), or coercion, "where a powerful state (or coalition of states with convergent interests)" forces other states to engage in a consistent practice benefitting the powerful state. *Id.* at 1114–15. The development of CIL to address State actions over social media would ideally be based on coordination, cooperation, or a coincidence of interest rather than coercion.

315. A clear formulation of the rule, its boundaries, recent developments, and application to cyber operations can be found in the Tallinn Manual. TALLINN MANUAL, *supra* note 308, at 312–25.

316. The "security dilemma" concept is again helpful here. In a "security dilemma," there is uncertainty over whether a State's actions will be perceived as defensive or offensive and escalatory. An accepted international norm against a particular action would reduce that uncertainty, allowing States to properly predict risk. For more information, see the discussion of offensive and defensive actions, *supra* notes 13 and 81, and the discussion of the "security dilemma," *supra* notes 82 and 14.

317. According to Professor Louis Henkin, the influence of international law need not be assessed by counting violations alone; the success of international law should also be measured by counting the times it was observed:

> There is a tendency to judge law observance by counting the violations, or, without counting them, from a general sense that they are common. But the influence of international law can hardly be assessed by the number of violations alone . . . . Also relevant is the record of law observance—decisions not to commit violations, failures to do so, and decades of diplomacy in which a nation does not even consider violating some norm or obligation.

HENKIN, *supra* note 311, at 46–47.

courts, and voters evaluate the rationale behind legislation. Shared language for discussing acceptable conduct also reduces friction for international coordination. This can enable parallel actions, such as sanctions or coordinated platform guidance.[318] Coordinated action backed by international norms may reduce the amount of deterrence needed (in other words, it may reduce the number of ex ante responses). International norms also guide responses, keeping them proportionate to the violation. Finally, international norms can raise reputational costs. Even without a standing tribunal, the "internationally wrongful" label can alter the strategic calculus of repeat offenders over multiple interactions.[319]

2. Evolution of the Rule Against Intervention

The rule crystallized in *Nicaragua v. United States*, where the International Court of Justice ("ICJ") coined the term "prohibited intervention" to describe actions as internationally wrongful, even if they did not involve a use of force.[320] The ICJ determined that the United States' support of the Contras, a rebel group opposing the recognized government of Nicaragua, was a prohibited intervention.[321] The elements of a prohibited intervention, according to the ICJ, are (1) the action must affect "matters in which each State is permitted, by the principle of State sovereignty, to decide freely" (also known as the *domaine réservé*), and (2) it must use "methods of coercion in regard to such choices."[322] As examples of matters in the *domaine réservé*, the ICJ listed "the choice of a political, economic, social, and cultural system."[323]

The *Nicaragua* case also illustrates the power of CIL as an example of a State acknowledging a CIL rule even though it initially worked against them. The United States was unhappy with the outcome of the case and even withdrew from the compulsory jurisdiction of the ICJ during the proceedings.[324] Since then,

318. Assurance games are further discussed in note 15 *supra*.

319. Henkin discussed the impact of reputation and repeated interactions on States' observance of international law: "Every nation's foreign policy depends substantially on its 'credit,'—on maintaining the expectation that it will live up to international mores and obligations." HENKIN, *supra* note 311, at 52. For an in-depth framing of this problem as a repeated game, see George Norman & Joel P. Trachtman, *The Customary International Law Game*, 99 AM. J. INT'L L. 541, 542 (developing "repeated multilateral prisoner's dilemma" model to explain adherence to CIL).

320. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 107–108 (¶ 205) (June 27) [hereinafter Nicaragua v. U.S.]. The ICJ relied on United Nations General Assembly Resolutions and other declarations. For example, Resolution 2625 states: "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State." G.A. Res. 2625 (XXV), annex, princ. 3, ¶1 (Oct. 24, 1970). For a detailed history of the principle of non-intervention, see Ori Pomson, *The Prohibition on Intervention Under International Law and Cyber Operations*, 99 INT'L L. STUD. 180 (2022).

321. Nicaragua v. U.S., *supra* note 320, ¶ 241 (finding the U.S. intention in supporting the Contras was to coercively interfere with the sovereign affairs of Nicaragua); *id.* ¶ 242 (U.S. "financial support, training, supply of weapons, intelligence and logistical support" were prohibited interventions).

322. *Id.* ¶ 205.

323. *Id.*

324. WEINER, HOLLIS & KEITNER, *supra* note 310, at 379–80.

however, U.S. legal scholars and government representatives have recognized a rule against intervention, even if the United States has not always behaved accordingly on the world stage.[325]

As technology and modes of intervention have evolved, government officials from the United States and the United Kingdom offered opinions on actions over the internet that could be considered prohibited interventions. They identified interference with the ability to hold an election, interference with legislative functioning, and interference with the State's ability to protect citizens' health as possible prohibited interventions.[326] As part of this discussion, some officials have espoused definitions of "coercion" that are broader than the use of force or the threat of use of force.[327] Since there is scant public evidence of State practice

325. Brian Egan, State Department Legal Advisor during the Obama Administration, and Paul Ney, Department of Defense (DoD) General Counsel during the first Trump Administration, both recognized a prohibition on intervention in speeches delivered during their tenure. Brian Egan, Legal Advisor, Remarks on International Law and Stability in Cyberspace (Nov. 10, 2016) (transcript available at https://perma.cc/4HW6-C48V) (calling non-intervention a "rule of customary international law") [hereinafter Egan Remarks]; Paul Ney, General Counsel to the Dep't of Def., Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020) (transcript available at https://perma.cc/EXC4-BWF9) (referring to an "international law prohibition on coercively intervening in the core functions of another State" and the "principle of non-intervention"). *See also* William Ossoff, *Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace*, 62 HARV. INT'L L. J. 295, 312 (2021) (discussing the Egan and Ney speeches while deducing U.S. recognition of a non-intervention rule). DOD LAW OF WAR MANUAL, *supra* note 308, § 17.18.1, recognizes a duty of non-intervention that would "require States to refrain from supporting non-State armed groups in hostilities against other States." In the Tallinn Manual, the International Group of Experts, which included U.S. representation, agreed "that the prohibition of intervention is a norm of customary international law." TALLINN MANUAL, *supra* note 308, at 312. The Tallinn Manual lists several other examples of U.S. express or implied endorsement of the prohibition of intervention. *Id*. at 312 n.761.

326. *See*, *e.g*., Egan Remarks, *supra* note 325; Jeremy Wright, U.K. Attorney General, Speech on Cyber and International Law in the 21st Century (May 23, 2018) (transcript available at https://perma.cc/JW5B-XCWA) (noting both "intervention in the fundamental operation of Parliament" and intervention in "the stability of our financial system" as potential prohibited interventions); Caroline Krass, General Counsel to the Dep't of Def., DoD General Counsel Remarks at U.S. Cyber Command Legal Conference (Apr. 18, 2023) (transcript available at https://perma.cc/8CK8-KWAT) (listing "coercive interference in a State's ability to hold an election or to protect the health of its population") [hereinafter Krass Remarks]; Suella Braverman, U.K. Attorney General, International Law in Future Frontiers (May 19, 2022) (transcript available at https://perma.cc/7CEP-B6T7) (including, among other scenarios, coercive interference with a "free and open election.") [hereinafter Braverman Remarks]. The United States' 2021 submission to the United Nations about the definition of "prohibited interventions" stated such interventions include interference with the ability to hold an election, manipulation of election results, and interference with the ability to protect the health of the population (for example, by interfering with vaccine research). *See* G.A. Res. 76/136, at 139–40 (Jul. 13, 2021). For further discussion of remarks by Egan, Braverman, and others, see Lauren M. Cherry & Peter P. Pascucci, *International Law in Cyberspace*, AM. BAR ASS'N (Jan. 27, 2023), https://perma.cc/N5G2-SPDA.

327. Caroline Krass discussed two possibilities while she was the DoD General Counsel: either causing a State to take an action it would not otherwise take or interfering with the State's "freedom of control," even if no compelled action can be identified. Krass did not endorse either definition, calling the question "ripe for further examination." Krass Remarks, *supra* note 326. Suella Braverman endorsed the second, broader approach while she was the U.K. Attorney General. *See* Braverman Remarks, *supra* note 326.

regarding prohibited interventions,[328] these officials' statements are important sources of the state of the law.[329]

Scholars have also proposed broader definitions that could encompass actions committed in cyberspace. As Gary Corn summarizes, strategic covert deception that is intended to deprive States of free will over matters in their *domaine réservé* may also be coercive; Russia's covert interference in the 2016 election is arguably an example of this.[330] Corn analogizes to the role of deception in domestic legal regimes, where there is "recognition that deception can substitute constructively for the actual force and coercion elements of other crimes."[331] Coercion through deception in the information environment involves subtler efforts to prevent a policy's implementation, destabilize political institutions, or manipulate public opinion in covert ways, thereby subverting a State's free will.[332] In the context of the social media manipulation we discussed above, this might include coordinated disinformation campaigns, false-identity operations, or amplification of false narratives.[333] While the collection of private information, by itself, would not be a prohibited intervention, a State's use of that information to manipulate the population of a target State may cross that line.

3. Applying the Rule Against Intervention to Recent Manipulation Concerns

The rule against intervention can be used to analyze anticipated or feared Chinese actions over TikTok, Russian election interference, and misinformation during the pandemic. During the debate over PAFACAA, lawmakers expressed a concern that China could compile information about Americans based on their TikTok activity and eventually use that information to blackmail government officials.[334] In the extreme, this could amount to a prohibited intervention by preventing

328. *See* TALLINN MANUAL, *supra* note 308, at 3 ("[B]ecause State cyber practice is mostly classified and publicly available expressions of *opinio juris* are sparse, it is difficult to definitively identify any cyber-specific customary international law.").

329. Even though traditional sources of CIL do not discuss cyber operations, the Tallinn Manual concludes this "does not mean, however, that cyber operations exist in a normative void." *Id*.; *see also* U.N. Int'l Law Comm'n, Draft Conclusions on Identification of Customary International Law, with Commentaries, U.N. Doc. A/73/10, Draft Conclusion 20, at 140 (2018) (including "public statements made on behalf of States; official publications; [and] government legal opinions" as evidence of *opinio juris*).

330. GARY P. CORN, COVERT DECEPTION, STRATEGIC FRAUD, AND THE RULE OF PROHIBITED INTERVENTION 4, 13–14 (2020), https://perma.cc/DMZ7-VKNS. Professor Corn is the director of the Technology, Law, and Security Program at American University's Washington College of Law and previously served as the staff judge advocate for U.S. Cyber Command. *Id*. at 28.

331. *Id*. at 3, 14.

332. *See id*. at 1–2, 11–15.

333. *Id*. at 4–6.

334. The possibility of blackmail was listed as a rationale in the 2020 EO requiring TikTok divestment. EO 13942, *supra* note 128, ¶ 3. Senator Mark Warner said, "[T]hat funny or inappropriate video two, five years from now, if somebody's trying to blackmail you from the Chinese spy services, I don't think you're going to want that to happen." TikTok Joint Appendix, *supra* note 65, at 362. In an interview with the New York Times, Rep. Mike Gallagher analogized TikTok to Grindr, which was the subject of a CFIUS-mandated divestiture due to its sensitive user data, as discussed *supra* Section III. B.2. Jane Coaston, *What the TikTok Bill is Really About, According to a Leading Republican*, N.Y.

America's government from representing Americans' interests. Lawmakers also voiced concern over election manipulation. Election manipulation could amount to a prohibited intervention if a State used its access to social media users and knowledge of their interests and motivations to destroy trust in an election, interfering with a State's ability to hold elections. For example, Russia sought to interfere in the 2016 elections by promoting divisive social issues, posting inflammatory content, and organizing rallies, among other tactics.[335] This interference took place over American-owned social media, and the effects may not be severe enough to qualify as a prohibited intervention. However, if the interfering State finds a large proportion of the target country's population on media platforms that it controls, manipulation may be easier and more effective. The Government argued in the recent TikTok litigation that ByteDance employees could promote content via TikTok that favored their preferred electoral outcomes, undermining the organic election process.[336] TikTok demonstrated a unique ability to influence voters during the debate over PAFACAA. Representative Mike Gallagher cited TikTok's mobilization of users to overwhelm Congress with angry communications in response to the ban as evidence of TikTok's influence over State decision-making.[337]

The PAFACAA debate also prominently featured concerns about TikTok's effect on public health. Members of Congress expressed concern that TikTok promotes harmful health content, whether or not intended as interference.[338]

TIMES (Apr. 1, 2024), https://perma.cc/XF93-Q8GU. Mr. Blackburn, the intelligence official discussed in note 65 *supra*, provided context to these concerns, describing China's "extensive and years-long efforts to accumulate structured datasets, in particular on U.S. persons, to support its intelligence and counterintelligence operations." TikTok Joint Appendix, *supra* note 65, at 634.

335. *See* 1 ROBERT S. MUELLER, III, U.S. DEP'T OF JUST., REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 14, 22–31 (2019). *See also* CORN, *supra* note 330, at 4 ("Russia's efforts in 2016 were aimed directly at the US presidential election. The objective was to undermine public faith in the democratic process . . . . Russia employed a multifaceted approach to its interference campaign that involved cyber espionage against both political parties; the weaponization of sensitive information collected through those operations, specifically the timed release through intermediaries of personal emails and other damaging information.").

336. Public Redacted Brief for Respondent, TikTok Inc. v. Garland, 122 F.4th 930, 2024 WL 3551836, at *37–38 (D.C. Cir. July 26, 2024) (promoting is also referred to as "heating").

337. *See* Coaston, *supra* note 334 (Rep. Gallagher said: "I think the push notification they forced on millions of users actually sort of proved our point about the concerns with how the tool could be weaponized to inject disinformation into the American legislative process and the democratic process."); Cristiano Lima-Strong & Drew Harwell, *TikTok Users Flood Congress with Calls as Potential Ban Advances in House*, WASH. POST (Mar. 7, 2024), https://perma.cc/V35B-MFY4. As further support for this concern, a study showed China creates election-related content on TikTok and other platforms meant to appear as if generated by Americans. *The #Americans*, GRAPHIKA 4 (2024), https://perma.cc/235H-QTX4. One study showed that frequent TikTok users were more likely to hold positive views of China, further evidence of the app's power to manipulate. *See* Finkelstein, et al., *supra* note 66, at 10, 21 (finding "anti-China sentiment" on TikTok to be significantly lower than on Instagram and YouTube, and those Americans who used TikTok for more than three hours a day to have a "49% increase in positivity towards China's human rights record.").

338. Members of Congress pointed to harmful health information provided by TikTok about eating disorders, self-harm, and Covid treatments, among other issues, in supporting PAFACAA. *TikTok Congressional Hearing*, *supra* note 135 (statement of Rep. Cathy McMorris Rodgers) ("Within minutes of creating an account, your algorithm can promote suicide, self-harm, and eating disorders to children. It encourages challenges for them to put their lives in danger."); *id*. (statement of Rep. Diana DeGette)

Promotion of false health information over social media, such that many people are induced to make dangerous health decisions, can prevent a State from protecting its population's health—and in extreme cases, amount to a prohibited intervention. U.S. officials have recognized "protect[ing] the health of the population" as part of the *domaine réservé*,[339] and severe misinformation campaigns that deprive the government of control over the population's health might amount to coercion. For example, according to the State Department, the Russian government created and promoted stories and memes attempting to amplify skepticism in America about American-made Covid vaccines.[340] If the campaign had been widespread and effective enough to lead many Americans to make poor personal decisions, it would have interfered with federal, state, and local efforts to protect vulnerable individuals.[341]

Governments can develop the definition of a prohibited intervention by refraining from actions they consider prohibited and publicly stating that they view those actions as violations of international law. A State committing a recognized prohibited intervention would invite countermeasures and international condemnation.[342] The affected State could use the "prohibited intervention" label to explain the need for a response to its population and its allies. As discussed, international recognition that these actions are prohibited allows the affected State to presume the action is offensive and puts the offending State on notice that the

("Another study showed that TikTok . . . had a hydroxychloroquine tutorial on how to fabricate this from grapefruit. . . . Number one, hydroxychloroquine is not effective in treating COVID . . . . The second issue is you can't even make hydroxychloroquine from grapefruit."); *id*. (statement of Rep. Raul Ruiz) ("The Journal of American Medical Informatics Association found that, when searching 'coronavirus' on TikTok, almost 30 percent of the videos that came up contained misinformation."). These messages could in total interfere with a country's ability to protect its population's health.

339. Krass Remarks, *supra* note 326.

340. Michael R. Gordin & Dustin Volz, *Russian Disinformation Campaign Aims to Undermine Confidence in Pfizer, Other Covid-19 Vaccines, U.S. Officials Say*, WALL ST. J. (Mar. 7, 2021), https://perma.cc/ETF2-K5K4; Julian E. Barnes, *Russian Disinformation Targets Vaccines and the Biden Administration*, N.Y. TIMES (Aug. 5, 2021), https://perma.cc/WA4M-X8UU.

341. The number of people who medically needed a vaccine but changed their minds because of Russian disinformation is unknown. However, it is possible to imagine an operation at a greater scale that creates widespread mistrust in a necessary medical treatment. In that case, the operation would prevent the government from carrying out a governmental function, i.e., protecting the population's health. This was not the only recent attempt by other countries to spread misinformation affecting population health. U.S. officials, early in the pandemic, accused Russian actors of running a coordinated campaign across thousands of accounts to spread false claims (e.g., that the virus was a Central Intelligence Agency bioweapon), which they warned could hamper outbreak control. Jessica Glenza, *Coronavirus: US Says Russia Behind Disinformation Campaign*, GUARDIAN (Feb. 22, 2020), https://perma.cc/H38Z-2C8K. Chinese accounts also spread the theory that Covid was engineered at a U.S. Army lab in Fort Detrick, MD, which could undermine trust in government efforts to curb Covid. *See* Legu Zhang, *China's Bogus Attack on a Top U.S. Coronavirus Lab*, VOA (Sep. 23, 2021), https://perma.cc/3BBD-96CK (Voice of America article countering China's efforts). Russia's efforts to criticize vaccines in the United States contrasted with Russia's efforts to promote its own vaccines in Serbia. Katrina Keegan, *Clarity for Friends, Confusion for Foes: Russian Vaccine Propaganda in Ukraine and Serbia*, HARV. KENNEDY SCH. MISINFORMATION REV. (Apr. 25, 2022), https://perma.cc/K5L7-7J3K.

342. *See* TALLINN MANUAL, *supra* note 308, at 111.

action will be perceived as such; this raises the expected costs of committing such actions.[343] When CIL is used to establish norms, a stable equilibrium is more likely to emerge, yielding greater overall benefit.[344]

4. Benefits and Drawbacks of Pursuing a Rule Against Intervention

Embrace of a rule against intervention can complement bans or regulations. If a rule against intervention successfully changes norms, States may avoid worst-case outcomes as their opponents refrain from the most extreme forms of manipulation. Such a rule provides diplomatic leverage and establishes expectations for how violations will be perceived. Moreover, States can use the "prohibited intervention" label to explain their responses to domestic audiences. Developing international law also carries the benefit of protecting all countries, not just those that have adopted domestic legislation. This reinforces the broader case for coordinated legal frameworks over reactive, one-off responses seen in the prior sections of this article.

This avenue comes with the drawback that development of CIL is hard, and its enforcement is even harder. Since the development of CIL requires consistent practice across States (even if not always followed), this solution rests on an assumption that States can sufficiently coordinate their statements and actions to hew to a norm (even if they do not reach any written agreements). Complicating matters further, this is an area in which State practice is likely to be hidden and *opinio juris* even harder to establish. Statements of experts from certain countries may not be sufficient to persuade the world of the expansion of this rule. Even if willpower-sapping manipulation over social media were accepted as a prohibited intervention, States might have difficulty reacting with proportionate countermeasures. International bodies likewise have difficulty enforcing CIL. Many prominent actors are not subject to the jurisdiction of bodies that can enforce it; for example, China, Russia, and the United States do not accept the ICJ's compulsory jurisdiction.[345] Still, these drawbacks do not prevent States from promoting a

343. This mitigates the uncertainty driving the "security dilemma." *See supra* notes 82 and 14.

344. Norman & Trachtman, *supra* note 319, at 562–65, provide several examples of CIL rules that can be seen as the result of a multilateral prisoner's dilemma. For example, the principle of territorial sovereignty and accompanying prohibition on the acquisition of territory by force has become stronger over the past century. Each State has "incentives to retain flexibility to acquire territory through the use of force" but "also wishes—defensively—to remove the flexibility of other states." *Id*. at 564. Through a CIL rule against acquiring territory, States reach a new stable equilibrium. *Id*. The authors show that the same principle applies to cross-border environmental harm, territorial jurisdiction, and restrictive sovereign immunity. *Id*. at 562–64.

345. Charter of the United Nations and Statute of the International Court of Justice, Declarations Recognizing as Compulsory the Jurisdiction of the International Court of Justice Under Article 36, Paragraph 2, of the Statute of the Court (Oct. 15, 1946), https://perma.cc/DS9L-UZJN. There is no international court that can prevent the countries discussed in this article from committing prohibited interventions over social media. It is possible that aspects of the TikTok dispute, including the U.S. decision to order divestment, could be brought to the World Trade Organization (WTO). In 2020, China claimed at a WTO meeting that TikTok restrictions were against WTO rules but never brought suit at the WTO. *China Says U.S. TikTok, WeChat Bans Break WTO Rules*, REUTERS (Oct. 5, 2020), https://perma.cc/DVT4-UVFV.

new understanding of the rule for the social media age or from using it to back up their domestic strategies. As Louis Henkin observed, international law exists even if there is no executive authority to enforce it.[346]

B. International Guidelines

In addition to the development of international law rules, the adoption of guidelines (voluntary, non-binding international instruments) might lead to more uniform responses to surveillance threats and easier adaptation for companies. "Soft law" principles and standards, which influence State behavior and corporate practices by articulating collective expectations, including benchmarks for responsible conduct, have the potential to shape the global environment surrounding surveillance. Norms-based tools provide the scaffolding for future supranational treaties, regulatory cooperation, adjudications, legislative reforms, corporate compliance strategies, and diplomatic dialogue.

The OECD Privacy Guidelines offer a compelling example of how to establish international norms around data collection and use—norms that could, especially if extended in future OECD Guidelines, be adopted by countries in their domestic legislation, and enforced, begin to constrain foreign intelligence gathering through social media apps.[347] The preamble establishes norms by recognizing "the fundamental values of privacy, individual liberties, and the global free flow of information," and recommending that member countries commit to the "protection of privacy."[348] Although framed to address commercial and governmental uses of personal data in a privacy-focused way, many of the Guidelines' core principles—such as collection limitation, purpose specification, use limitation, security safeguards, and individual participation[349]—challenge the legality of

---

346. Louis Henkin was a professor at Columbia Law School and an influential international law scholar. He observed:

> The impression that nations commonly violate international norms and undertakings may be due not only to incomplete observation, but also to erroneous *a priori* assumptions about how nations behave. Much is made, in particular, of the lack of executive authority to enforce international law and the lack of effective 'sanctions' against the violator. The assumption seems to be that since law and agreements limit the freedom of nations, governments will not observe these obligations, unless they are compelled by external authority and power. In fact, we know—although effective 'sanctions,' as that term is commonly used, are indeed lacking—that nations do generally observe laws and obligations.

HENKIN, *supra* note 311, at 49.

347. *See generally* Organization for Economic Cooperation & Development [OECD], *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD/LEGAL/0188 (Sep. 29, 1980, as amended July 11, 2013), https://perma.cc/8PWV-QHK9.

348. *Id.* pmbl., § 1.

349. The Guidelines establish principles for "data controllers," parties that make decisions about collection and use of personal data. *Id.* Annex ¶ 1(a). In other words, if the OECD members implement the Guidelines' principles, domestic law in those countries would follow the principles by imposing limits on companies and government agencies that collect personal data. The Collection Limitation Principle recommends "limits to the collection of personal data," which must be "obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject." *Id.* ¶ 7. The

indiscriminate surveillance practices or surveillance in which the target is never notified.[350] In particular, however, the insistence that data be collected only for legitimate, specified purposes and not reused for other ends without consent could dissuade States from engaging in sweeping intelligence gathering through app ecosystems.[351] By encouraging free data flows between member countries if those countries protect privacy rights, the Guidelines aim to build trust.[352] This could counteract the trend of escalating restrictions in response to threats seen in the unilateral responses above.

The OECD model has influenced national privacy legislation—especially in the EU, Japan, and increasingly in U.S. state laws—and has set a benchmark with which surveillance practices are increasingly in conflict.[353] Surveillance conducted via social media apps, cloud services, and mobile platforms often circumvents or undermines the expectations these frameworks create. The OECD's more recent efforts—such as the Recommendation on Enhancing Access to and Sharing of Data—are further examples of the promotion of rights-respecting cross-border data use.[354]

OECD Guidelines, in the most optimistic scenario, could encourage privacy-focused changes to domestic law that would constrain intelligence agencies: in other words, a sort of "arms reduction treat[y] for intelligence surveillance," as

---

Purpose Specification Principle requires, "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes." *Id.* ¶ 9. The Use Limitation Principle limits use of personal data to those purposes which were specified to the subject at the time of collection, unless "by the authority of law." *Id.* ¶ 10 (b). While there is an argument that the "compelled by law" provision legitimizes use of data by State intelligence agencies consistent with those States' laws, this at least encourages clear laws delimiting when data can be used by government actors. The Security Safeguards principle requires data to be protected from "unauthorized access." *Id.* ¶ 11. The Individual Participation Principle requires an individual to be able to request all data on them from the data controller. *Id.* ¶ 13.

350. While the target of surveillance is rarely notified while they are being actively monitored, some surveillance regimes require notice to the target in all cases after surveillance has concluded, bringing surveillance in these regimes into greater alignment with the Guidelines' Purpose Specification Principle and Collection Limitation Principle. For example, the Wiretap Act contemplates no-notice interception but mandates a post-interception "inventory" notice. "Within a reasonable time but not later than ninety days" after the interception order has terminated or the application for an interception order has been denied, the responsible judge must ensure this notice is served. 18 U.S.C. § 2518(8)(d). The Stored Communications Act also builds notice into compelled-disclosure provisions. *Id.* § 2703(b)(1)(B). Section 2705 authorizes delayed notice for up to ninety days (with extensions) where notice would risk specified adverse results. *Id.* § 2705(a)(1), (a)(4)–(5).

351. *See, e.g.*, *id.* ¶¶ 7, 9, 10, 12.

352. The Guidelines state, "A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist." *Id.* ¶ 17. The Guidelines also frame any surveillance-based restrictions through a proportionality lens: "Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing." *Id.* ¶ 18.

353. *See* ORG. FOR ECON. COOP. & DEV., THE EVOLVING PRIVACY LANDSCAPE: 30 YEARS AFTER THE OECD PRIVACY GUIDELINES, 13–14 (Apr. 6, 2011), https://perma.cc/V798-U4MT.

354. OECD, *Recommendation of the Council on Enhancing Access to and Sharing of Data*, OECD/LEGAL/0463 (May 10, 2021), https://perma.cc/G9C4-KS57.

posited by Julian Sanchez.[355] By extending reciprocal procedural protections to the citizens of allied states, countries could begin to re-anchor intelligence cooperation in norms of mutual restraint and accountability. Such a framework is not unprecedented: the Obama Administration's Presidential Policy Directive 28 (PPD-28), the Biden Administration's EO 14086, and proposals for an "Algorithmic Rights Court" are examples of where a push for transparency and redress for foreign citizens was politically possible.[356] OECD principles could gradually normalize new rules of engagement in the intelligence realm. While difficult to verify and less likely to gain traction among authoritarian regimes,[357] the existence of hard cases should not preclude the development of soft rules.

Another example of international law development related to cyber communications is the United Nations Convention Against Cybercrime.[358] The General Assembly passed the Convention Against Cybercrime on December 24, 2024.[359] It opened for signatures on October 25, 2025.[360] Although negotiations toward this convention were difficult, and the convention has been criticized for advancing the interests of its initial sponsor, Russia, the convention provides an example of how international law may yet be a pragmatic near-term path.[361] Some of the

355. Julian Sanchez, *TikTok, Schrems II, and Cross-Border Data Flows*, CATO INST. (July 6, 2021), https://perma.cc/JY2L-3YD7. Widespread adaptation of privacy-focused guidelines to deescalate intelligence surveillance would be an example of successful coordination in an assurance game. *See* discussion *supra* note 15.

356. PPD-28 recognized the privacy rights of non-U.S. citizens in data collected by U.S. intelligence agencies. *See* Presidential Policy Directive—Signals Intelligence Activities, 2014 DAILY COMP. PRES. DOC. 31 (Jan. 17, 2014), https://perma.cc/KJ6V-T9DM ("all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information."). As discussed, EO 14086 establishes a mechanism for citizens of certain nations to lodge complaints regarding the handling of their data. EO 14086, *supra* note 50; *see* discussion *supra* note 267. The EO is noteworthy for granting non-U.S. citizens remedies regarding their data privacy, even though little information exists on the effectiveness of these remedies. *See also* Ira Rubinstein & Peter Margulies, *Risks and Rights in Transatlantic Data Transfers: EU Privacy Law, U.S. Surveillance, and the Search for Common Ground*, 54 CONN. L. REV. 391, 398 (2022) (proposing an "Algorithmic Rights Court (ARC) that will field EU persons' privacy complaints. The ARC would be staffed by life-tenured federal judges and aided by a full-time public advocate to push back on government positions. It would provide gold-standard independent review.").

357. Jacques deLisle, *Security First? Patterns and Lessons from China's Use of Law to Address National Security Threats,* 4 J. NAT'L SEC. L. & POL. 397, 398 (2010) (discussing how China has "engaged international legal norms").

358. G.A. Res. 79/243 (Dec. 24, 2024).

359. *Id.*

360. As of January 3, 2026, the convention had 74 signatories, including China, Russia, the EU, and the U.K.; the United States has not signed. *Status of Treaties: United Nations Convention against Cybercrime*, U.N. TREATY COLLECTION (Jan. 3, 2026), https://perma.cc/TR7D-DAKS; *see also* U.N. Off. of Drugs & Crime, *United Nations Convention Against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes*, UNITED NATIONS, https://perma.cc/D5LJ-KUTM.

361. Alexander Seger, *Russian Motivations Behind the "Hanoi Convention" Against Cybercrime*, JUST SECURITY (Oct. 7, 2025), https://perma.cc/LN8X-EF94; *see also* Vibhu Mishra, *UN General Assembly Adopts Milestone Cybercrime Treaty*, UNITED NATIONS (Dec. 24, 2024), https://perma.cc/

convention's provisions on illegal data access could require states to adopt laws that would forbid State-conducted interception or interference operations, but they are not specifically designed to address the sovereignty, surveillance, and nonintervention concerns at the heart of this article.[362] It is important to implement parallel norm-building efforts for social media surveillance.

C. Lessons from this Approach

The two approaches observed here, application of CIL and development of guidelines, both carry the advantage of more universal reach. For example, if CIL were developed such that election interference via social media were recognized as a prohibited intervention, States may be deterred from carrying out such an intervention against any other State. If the OECD Guidelines were implemented by OECD members as well as other countries, States would implement privacy protections for everyone's data and not just the data of their own citizens. Both developments would help avoid tit-for-tat responses.

By encouraging all countries to respect privacy and national sovereignty in the administration of data collected by their social media companies, international rules or norms have the potential to stop the problem at its source. Individuals benefit from greater personal privacy. In that ideal world, States would not need to censor applications. In the real world, where international law is not always followed or enforced, and non-binding guidelines are even less likely to be followed, this approach still complements domestic law. Even if bad behavior is not totally dissuaded, the cost of that behavior to the offending State increases. Additionally, the State fending off a threat can explain the threat to its citizens and to other countries using the language of international law. This could reduce the perception of protectionism and facilitate cooperation across borders.

Relying on international rules and norms may help resolve the tension over how different legal systems enshrine rights. Europe has elevated privacy to a quasi-constitutional status. In the United States, by contrast, constitutional protections extend to free speech (as in TikTok's case) and Fourth Amendment limits on government searches (which notably do not protect non-USPs abroad) but not to data privacy. This asymmetry means that when EU and U.S. laws intersect, any resulting conflict effectively pits a fundamental right to data privacy against sovereign interests in security and expression.

As discussed, international rules and negotiated guidelines do not solve everything. CIL rules, such as the prohibition on intervention, even if developed to incorporate interference over social media, would likely only address the most egregious cases (e.g., widespread blackmail of government officials or undermining faith in the electoral process). CIL rules and negotiated guidelines are both difficult to enforce. Without an enforcement mechanism constraining States' options, States' commitments to follow rules or guidelines may lack credibility.[363]

ZFA9-RVDD; *Panel Shares Insights on Drafting New U.N. Cybercrime Treaty*, YALE L. SCH. (Apr. 8, 2025), https://perma.cc/ZD78-B3GA.

362. *See, e.g.*, G.A. Res. 79/243, *supra* note 358, arts. 7–13.

363. The "credible commitment" problem is discussed in note 19 *supra*.

One salient drawback of the OECD Guidelines is that the OECD only incorporates 38 member states.[364] Russia and China are not among them. While the Guidelines may be persuasive for some member states, they will not rein in major surveillance threats like Russia and China. As a result, they cannot stop the reactive dynamic of cyber threats and responses. Further, the Guidelines have been insufficient to persuade all member states to stop surveilling non-citizens' data. For example, as discussed, U.S. law recognizes few, if any, privacy rights for non-USPs abroad. Australia, also an OECD member, is another example: Australian law governing data collection for intelligence purposes recognizes privacy rights for Australians, but not for citizens of other countries.[365] This highlights that any guidelines only apply to the countries that have indicated an intention to follow them. It further illustrates that the development of both international rules and guidelines requires a high degree of coordination (or at least aligned interests), and there are incentives for all sides to defect from the optimal, cooperative solution.

Finally, this approach is especially tricky for countries like the United States, which are both targets of social media surveillance and have extensive intelligence-gathering capabilities. The United States' Five Eyes partners (Australia, the United Kingdom, Canada, and New Zealand) and other close allies sharing intelligence with the United States fall into the same category. These countries must balance their interest in preventing espionage and manipulation of public opinion with their own need to influence public opinion and gather intelligence. The development of international rules and norms may protect citizens who use social media but may also contradict intelligence practices of value to national security. The concept of a two-level game is helpful here: States' intelligence requirements and States' interests in their own data security exist at two different levels.[366]

Classification of State Responses to Foreign Digital Influence and Surveillance: *Spectrum from most to least restrictive*

Foreign-owned Platform Ban	Foreign-owned Platform Divestiture	Comprehensive Data Privacy Regulation	International Norm Development
India's TikTok ban *China's "Great Firewall"* *Ukraine's VK Group ban*	*PAFACAA (U.S. TikTok divestiture requirement)* *Executive branch, CFIUS-driven divestitures (Kunlun Tech & Grindr, iCarbonX & PatientsLikeMe)*	*GDPR (informing EU responses to FISA, TikTok, etc.)* *U.S. comprehensive data privacy proposals*	*Rule against prohibited interventions (ICJ)* *OECD framework & other advisory guidelines*

364. *Members and Partners*, ORG. FOR ECON. COOP. & DEV., https://perma.cc/45BN-6GSA.

365. *Office of National Intelligence Act 2018* (Cth) § 53 (Austl.), https://perma.cc/4TVS-9NFU ("Privacy rules to protect Australians"); Peter Dutton, *Rules to Protect the Privacy of Australians 2021*, AUSTRALIAN SIGNALS DIRECTORATE (Nov. 30, 2021), https://perma.cc/7MN9-RJS6.

366. This is similar to the two-level game of diplomacy and domestic politics discussed in Putnam, *supra* note 17.

V. CONCLUSION

This article described four categories of State responses to the threat of foreign interference over social media: outright bans, forced divestitures, comprehensive data privacy regulation, and international law development. These approaches can be further organized along a spectrum according to their effect on the social media platforms of concern—from most restrictive (completely banning certain platforms) to least restrictive (establishing guidelines for how platforms and States behave).

As seen in each of the cases discussed above, State responses are often reactive, directly shaped by the surveillance structures as described in Section II and by other countries' responses as described in Section III. For example, FISA spurred the GDPR, and China's laws spurred the Court's conclusion in *TikTok Inc. v. Garland*. Reciprocity compounds these dynamics, as States mirror one another's restrictions and regulatory models. The *Schrems* litigation prompted U.S. reform through EO 14086, and PAFACAA led to the consideration of similar measures in other countries. The classification of policy options proposed in this article lays the groundwork for analyzing the interactions between threats and responses using concepts from international relations game theory, a suggested area of future research.[367]

PAFACAA withstood the passionate opposition of American creators and powerful lobbying from ByteDance. Still, it remains to be seen whether it successfully neutralizes the threat of surveillance and manipulation over TikTok and other social media applications. In any case, there are benefits to comprehensive data privacy legislation and development of international norms. The United States should renew its focus on these as part of a complete solution. Comprehensive laws can limit the amount and sensitivity of data available for government access in the first place, making foreign surveillance more difficult no matter who controls the platform. Meanwhile, international norms help coordinate uniform cross-border expectations—reducing the risk of the worst-case scenarios, such as State-sponsored behavioral manipulation. Political, practical, and legal challenges, of course, may necessitate interim measures.

367. These concepts are discussed in notes 13–19 *supra*.