Out of Control—the United States Government's Ever Expanding Foreign Direct Product Rule (FDPR)

Charlynn M. H. Teter

Abstract

Comment discusses the recent and ongoing substantial expansion of the Foreign Direct Product Rule (FDPR) and evaluates the extent to which, as the scope of the FDPR expands, it is increasingly in tension with both international and domestic law. This Comment analyzes the viability of the available legal and procedural mechanisms, both international and domestic, to challenge or halt the FDPR's expansion. Finally, this Comment cautions that the low likelihood of companies seeking and prevailing on such relief suggests that further expansion of the FDPR is particularly troubling.

Table of Contents

I. INTRODUCTION

The Foreign Direct Product Rule (FDPR)[1] applies U.S. export controls to certain goods manufactured in and exported from foreign countries. First enacted in 1959 to target military products manufactured overseas, until 2019,[2] the FDPR controlled military items and satellites without significant controversy. These narrower versions of the rule barred sales (1) of products which the U.S. government identified as posing a national security risk that (2) were originally made using U.S. technology to (3) particular end destinations.[3]

In 2020, the first Trump Administration opened a Pandora's box, using[4] the FDPR as a tool to ban general commerce—including foreign products designed, made, and sold entirely overseas by non-U.S. persons—to specific entities.[5] This new FDPR rule controls products without regard to the end product—controlling all products that were (1) originally made, at least in part, with certain U.S. technology and were (2) exported to a listed party, whether or not the product itself is a national security threat.[6]

Without an end-product limit, the Entity List Rules (footnotes 1, 4, and 5 to the current FDPR, hereinafter, respectively, FDPR fn. 1,4,5),[7] apply to *all* products made using controlled U.S. technology and products made in factories that were made using controlled technology.[8] The rule prohibits any person worldwide (including non-U.S. persons) from selling nearly *anything* to Entity List companies, including products with no national security nexus: such as a Tesla automobile, a five-year-old Apple laptop, a Sony PlayStation, and a Nokia cellphone.[9] A European automaker cannot ship a sedan to any one of the hundreds of companies on the ever-growing FDPR list[10]—even if that sedan never touched an American person or American soil.

---

1 15 C.F.R. § 734.9.

2 Larry Sussman, *Seagate's $300M Lesson*, WIRESCREEN (Jan. 26, 2024), https://perma.cc/3RPJ-43K9.

3 *Id.*

4 *Id.*

5 Not to be confused with the UFLPA Entity List (Notice Regarding the Uyghur Forced Labor Prevention Act Entity List, 90 Fed. Reg. 3899 (Jan. 15, 2025)), which restricts *imports* from entities suspected of using forced labor practices; this FDPR Entity List restricts *exports* to entities which allegedly pose a national security risk to the U.S.

6 15 C.F.R. § 734.9(e).

7 *Id.*

8 *Id.* § 734.9(e).

9 15 C.F.R. §§ 734.9(e)(1)(i); 734.9(e)(2)(i); 734.9(e)(3)(i)(B)(2).

10 *Id.*

At first, the FDPR Entity List expansion seemed targeted to a narrow list of entities deemed national security threats, most notably, Huawei.[11] Using the FDPR to ban sales, shipments, and re-sales of nearly all products (even products that have no feasible connection to national security) did not trigger widespread alarm, because the *recipients* of those products—the parties on the entity list—appeared, by their very existence, to be national security threats.

But over the last several years, a rule that started as a narrow mechanism to target national security threats gradually expanded into something far broader—far reaching commerce regulation without judicial review or checks and balances. The Entity List has massively expanded—to date, it covers hundreds of companies[12]—and threatens to cover tens of thousands of "affiliate" companies. The "affiliates" rule, issued in late 2025, included any entities "affiliated" even indirectly with Entity List companies without making particularized assessments of whether any individual company was diverting sales.[13] The Trump Administration stayed[14] the Affiliates Rule as part of a bargain with China, but only temporarily.[15]

Especially with the "Affiliates Rule," the FDPR threatens to become so broad that it ceases to function as a national security tool. The rule is becoming a means to extract economic leverage, functioning contrary to international law, exceeding the authority of domestic law, and raising serious public policy concerns.

The U.S. government cites national security as its international law authority to restrict foreign trade (including foreign trade without any U.S. person involvement).[16] Indeed, the "protective principle" in international law recognizes that states may exercise extraterritorial jurisdiction to protect key national security interests.[17] International treaties to which the U.S. is a party which limit trade

---

11 Supplement No. 4 to Part 744, Title 15 (Apr. 9, 2026), p. 508 (Huawei is repeatedly referenced throughout Entity List due to many listed subsidiaries but see p. 508 for the inclusion of the company titled "Huawei Technologies Co., Ltd."); *U.S. targets Huawei with tighter chip export rules*, BBC (May 15, 2020) https://perma.cc/6UFX-MRQK.

12 Supplement No. 4 to Part 744, Title 15 (Apr. 9, 2026) [hereinafter Entity List].

13 Expansion of End-User Controls to Cover Affiliates of Certain Listed Entities, 90 Fed. Reg. 47201 (Sep. 30, 2025) [hereinafter Affiliates Rule].

14 One Year Suspension of Expansion of End-User Controls for Affiliates of Certain Listed Entities, 90 Fed. Reg. 50857 (Nov. 12, 2025) [hereinafter Suspension of Affiliates Rule].

15 Doina 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/SBK2-RAC8.

16 *Understanding the Extraterritoriality of U.S. Export Controls*, CTP, https://perma.cc/P8GD-ULXD (last visited Oct. 26, 2025) [hereinafter *Understanding the Extraterritoriality of U.S. Export Controls*].

17 RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 412 (A.L. I. 2018).

restraints also provide for national security exceptions.[18] Therefore, if the FDPR applied only to a narrow list of entities whose mere existence raise clear national security concerns, or if it implicated only end-products which have credible national security implications, it would not raise eyebrows. Such rules plausibly protect the U.S.'s national security interests.

However, increasingly, the new version of the FDPR's national security justification does not withstand good-faith scrutiny.[19] The plain text of the rule covers objects and products which have not been identified as national security threats; the U.S. government has imposed the new FDPR to a rapidly-growing, wide range of entities with substantial commercial, non-military, footprints;[20] and finally, the U.S. government has explicitly agreed to limit the imposition of FDPR expansions—in particular, the Affiliates Rule—in exchange for economic,[21] not security-based, concessions from foreign governments. No other legitimate bases for an extraterritorial exercise of U.S. jurisdiction apply. Therefore, FDPR fn. 1,4,5 likely violate—or will soon violate—international law.

Domestically, the Executive has the authority to regulate foreign trade to protect the U.S.'s national security interests under the Export Control Reform Act of 2018 (ECRA).[22] However, the increasingly broad FDPR fn. 1,4,5 may exceed the executive branch's statutory authority[23] to enact such regulations. ECRA does not *create* U.S. jurisdiction where none previously existed[24] and does not clearly contradict international law; therefore, it should be read to conform with international law's standards for establishing extraterritorial jurisdiction. Furthermore, ECRA is not a blank check for the Commerce Department to impose a worldwide embargo of all products of any entity it chooses: the statute explicitly requires that its implementation, when unilateral, be narrowly targeted[25] and achieve a balance that promotes U.S. economic interests and leadership.[26] Increasingly, the Entity List meets neither requirement.

---

18 *See, e.g.*, General Agreement on Tariffs and Trade, art. XXI, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194 [hereinafter GATT].

19 *See* Panel Report, *Russia—Measures Concerning Traffic in Transit*, ¶¶ 7.132–7.138, WTO Doc. WT/DS512/R (adopted Apr. 5, 2019) regarding "good faith" requirements [hereinafter Measures Concerning Traffic in Transit Report].

20 Entity List, *supra* note 11.

21 Chiacu & Alper, *supra* note 15.

22 Export Control Reform Act of 2018, 50 U.S.C. §§ 4811–4826.

23 *Id.*

24 50 U.S.C. § 4812(a)(1) (expanding the statute's grant of regulatory authority to cover only "items subject to the jurisdiction of the United States").

25 50 U.S.C. § 4811(6) (stating that "[a]pplication of unilateral export controls should be limited for purposes of protecting specific United States national security and foreign policy interests").

26 50 U.S.C. § 4811(3).

While the FDPR fn 1,4,5 is legally dubious both as a matter of international and domestic law, as a practical matter, challenging the rule is difficult. Foreign governments do not have a meaningful or effective forum to bring a claim—either internationally or within the U.S.'s domestic courts. Challenges brought within the U.S.'s domestic courts appear more viable, but given the power of the national security talisman, remain relative long shots. Impacted businesses or individuals could theoretically (1) bring *ultra vires* claims alleging that the executive branch has exceeded its statutory authority,[27] (2) challenge the validity of certain enforcement actions under the Administrative Procedures Act (APA),[28] or (3) bring constitutional challenges under the nondelegation doctrine—but none of those are likely to succeed.

But even if the FDPR is beyond legal challenge, U.S. regulators should ask whether they have reached the point of diminishing returns. The 1959–2019 framework was narrow and focused, preserving U.S. credibility and promoting U.S. interests worldwide. The current FDPR risks: (1) retaliation from other countries; (2) an increased international hesitancy to rely on U.S. products and technology; and (3) a deteriorating reputation for the U.S. internationally. A policy reversal is possible: although the first Trump Administration expanded the FDPR, nothing prevents the second Trump Administration from dialing the rule back.

II. Defining the Scope of the Foreign Direct Product Rule

The FDPR applies the export control rules which govern U.S. products to certain exports and in-country transfers of products made by non-U.S. nationals outside of the U.S.[29]

A. History of the FDPR

The FDPR began as a Cold War measure[30] and was "narrowly tailored to prohibit the sale of items subject to strict national security controls in the event they were produced overseas either as a direct product of U.S. technology or in a foreign factory utilizing U.S. technology."[31] The rule focused on national security

27 50 U.S.C. §§ 4811–4826, *supra* note 22.

28 5 U.S.C. §§ 551-559, 701–706.

29 *Update Conference on Export Controls and Policy: Partnerships in National and Global Security*, Bureau of Indus. & Sec. (Mar. 25, 2024) https://perma.cc/6CJG-327M [hereinafter *Update Conference on Export Controls and Policy*].

30 Sussman, *Seagate*, *supra* note 2.

31 *Id.*

and was not used to control commercial products.[32] Although the U.S. government amended the rule slightly between 1959 and 2020, the first substantial changes occurred during the first Trump Administration and continued thereafter under both President Biden and the second Trump administration.[33] The stated rationale for these substantive changes was concern over "dual-use technology," which has legitimate civilian and consumer uses but can also serve military functions.[34] To sweep in these technologies without enumerating them, the government substantially adjusted the limiting principles for new iterations of the Rule; removing end-product "output" requirements and relying only on "input" and "end-user" requirements to limit the scope.[35]

B. The Three-Prong Framework of the FDPR

Applying the FDPR depends on three factors: (1) the nature of the foreign-produced "output"; (2) the nature of the "inputs" used to make the foreign-produced product; and (3) the destination/end-user scope or who and what ultimately uses the product.[36] These first two factors are sometimes referred to as the "product scope."[37]

Older versions of the FDPR used all three factors to limit the Rule's application. For example, the long-standing "national security" FDP rule[38] restricts exports of products that: (1) are listed under the Export Control Classification Number (ECCN) system for national security reasons;[39] (2) are the direct product of controlled U.S. technology or the product of a factory that is itself the product of such technology (or which has a "major component that is

---

32 *Id.*

33 *Id.*

34 KAREN M. SUTTER, CONG. RSCH SERV., R48642, U.S. EXPORT CONTROLS AND CHINA: ADVANCED SEMICONDUCTORS, (2025).

35 15 C.F.R. § 734.9(e).

36 *Update Conference on Export Controls and Policy, supra* note 29.

37 *Id.*

38 15 C.F.R. § 734.9(b).

39 A very wide range of products have ECCNs assigned to them. The classification list includes, broadly: (1) nuclear materials, facilities, equipment, firearms, ammunition; (2) special materials, chemicals, microorganisms, and toxins; (3) materials processing; (4) certain electronics and computers; (6) telecommunications; (7) sensors and lasers; (8) navigation and avionics; (9) marine vessels and technology; and (10) aerospace and propulsion technology. Any product which falls within a narrower category identified on the list has a specific classification number assigned to it. In contrast, products which do not fall into a category that has been identified as particularly concerning are designated as "EAR99" items. *Interactive Commerce Control List*, BUREAU OF INDUS. AND SEC., https://perma.cc/Q5V5-8APN.

the product of such technology"); and (3) are destined for a country listed in Country Group D:1, E:1, or E:2.[40]

However, the Entity List FDPR has dramatically shifted the output (1) and end-user (3) criteria, resulting in an increasingly expansive rule.

1. The Product Scope—From a Narrow Focus on Weapons to anything Containing a Chip (Even Old Ones)

Most of the FDPR's provisions cover only certain kinds of final products.[41] Typically, the rules only apply if the final product produced overseas is subject to specific Export Control Classification Number (ECCN) designations, which can include military-grade technologies or any other items the U.S. government has specifically identified as national security threats.[42]

When considering **input**, two different criteria matter: the inputs or technology that produced the item, *and* the inputs or technology that produced the plant or factory that produced the item. First, if items are produced "directly" by the use of certain technology or software, that technology or software counts as an input.[43] Second, if the items were produced by a plant, then technology used to construct the plant or any major component of the plant also counts as an input—even if no U.S. technology is part of the final product.[44] A "major component" of the plant means "'equipment' that is essential to the 'production' of an item, including testing 'equipment.'"[45]

40 15 C.F.R. § 734.9(b).

41 15 C.F.R. § 734.9.

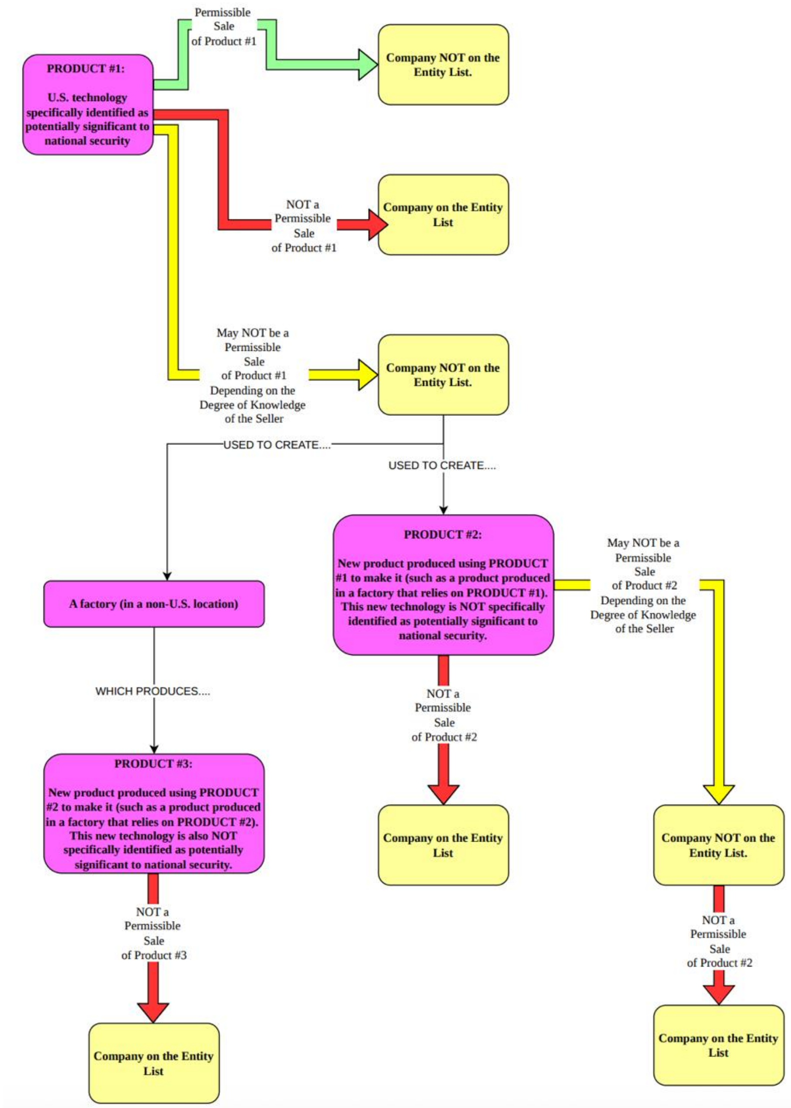
42 *Id.*

43 *Id.*

44 *Id.*

45 *Id* at § 734.9(a)(1)(i).

Therefore, the "input" prong is not a particularly strong limiting factor: it functions on a "contamination" principle (illustrated below), covering products only tangentially linked to U.S. inputs.



The end-product prong of the product-scope requirements therefore can be a far more significant limit on the Rule's scope than the input prong. Most of the nine different FDP rules' end-product requirements apply the rules only to limited products which the U.S. government has identified as risky to national security.[46] For example, the Advanced Computing FDP Rule[47] covers "sensitive computer-related items."[48] Its end-product scope restriction applies only to certain technology listed on the CCL (Commerce Control List),[49] such as "advanced chips" which reach certain combinations of Total Processing Performance and performance density.[50]

The Entity List provision of the FDP Rule (FDPR fn. 1,4,5) is unusual: the provision allows the government to regulate products whether or not the end product poses a security threat.[51] Given the lack of an end-product provision and a typically broad "contamination rule" input provision,[52] the "product scope" of the Entity List rule can cover items *not* identified as posing any intrinsic national security risks: old iPads, Roombas, Smart Fridges, GPS devices in cars, and many similar items. The proliferation of these products does not pose any national security risk: if they *did*, they would have been assigned a ECCN and would be directly controlled.

2. End User Scope—From a Narrow List to Tens of Thousands of "Affiliates"

The Entity List FDP Rule initially narrowly cabined the "End User" scope to a narrow list of companies identified as national security risks. However, this entity list has ballooned—and is continuing to balloon. Currently, the FDPR fn.1,4,5 "entity list" includes more than 150 entities affiliated with Huawei, nearly 100 entities that are alleged to support the PRC's "AI" ecosystem, and over a dozen integrated circuit fabrication facilities.[53] In the fall of 2025, the U.S. government added tens of thousands of companies via the "Affiliates Rule."[54] Although the government stayed the Affiliates Rule for a year, the U.S. recently announced that it intends to put the Affiliates Rule in effect in November 2026.[55]

The Affiliates Rule will dramatically expand the Entity List by including (1) companies which are 50% or more owned by a company on the entity list; (2)

---

46 *Id.*

47 *Id.* § 734.9(h).

48 *Update Conference on Export Controls and Policy*, *supra* note 36.

49 *Interactive Commerce Control List*, BUREAU OF INDUS. AND SEC., https://perma.cc/Q5V5-8APN.

50 Larry Sussman, *Regulating A.I. through the Supply Chain*, WIRESCREEN (Apr. 10, 2024), https://perma.cc/L46V-Z594.

51 15 C.F.R. § 734.9(e). *Contrast with* 15 C.F.R. § 734.9(b)–(d), (f), (h).

52 15 C.F.R § 734.9(e)(1)(i)(B), (e)(2)(i)(B).

53 Entity List, *supra* note 11.

54 Affiliates Rule, *supra* note 13.

55 Suspension of Affiliates Rule, *supra* note 14.

companies which are 50% or more owned *in the aggregate* by companies on the entity list; and (3) companies which are owned by any company qualified to be added to the list under (1) and (2).[56]

III. Drifting From The Original Moorings—The Legal Weaknesses of the New FDPR Entity List Rule

While many provisions of the Foreign Direct Product Rule (FDPR) are permissible under international law as justifiable national security measures, the increasingly broad and undifferentiated nature of FDPR fn. 1,4,5[57] is difficult to justify as a national security measure. Therefore, FDPR fn. 1,4,5 likely violates—or may soon violate—international law.

Furthermore, FDPR fn. 1,4,5 may plausibly violate domestic law by exceeding the authority granted to the executive branch under the ECRA.[58] The best reading of ECRA—based both on the text of the statute and the *Charming Betsy* canon—would read it to grant the Executive only a limited authority to constrain exports in a manner in line with international law. Under that more limited authority, the Executive would not have the authorization to impose FDPR fn. 1,4,5.

A. The expanded FDPR conflicts with international law

1. A version of the FDPR which, in good faith, protects national security concerns is permissible under international law

Extraterritorial restraints on trade potentially violate two types of international law: (1) principles of sovereignty, which limit where countries may enact prescriptive law; and (2) trade treaties between the U.S. and impacted countries. However, to the extent that extraterritorial restraints on trade are narrowly imposed to protect the regulating country's national security interests, both jurisdictional rules and trade treaties permit their imposition.

In accordance with international law, the U.S. usually asserts jurisdiction only "to prescribe law with respect to: (a) persons, property, and conduct within its territory; (b) conduct that has a substantial effect within its territory; (c) the conduct, interests, status, and relations of its nationals and residents outside its territory; (d) certain conduct outside its territory that harms its nationals; (e) certain conduct outside its territory by persons not its nationals or residents that

56 Affiliates Rule, *supra* note 13.

57 15 C.F.R. § 734.9(e).

58 50 U.S.C. §§ 4811–4826.

is directed against the security of the United States or against a limited class of other fundamental U.S. interests; (f) certain offenses of universal concern . . . ."[59]

The U.S. government relies on category (e) "national security,"[60] to justify the FDPR's trade restrictions:[61] "[d]espite objections, the U.S. maintains these measures as vital to countering threats like weapons proliferation and terrorism."[62] Category (e) essentially restates the general customary international law recognition of the "protective principle."[63] The "protective principle" describes "a state's jurisdiction to prescribe law with respect to certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other fundamental state interests, including espionage, certain acts of terrorism, murder of government officials, counterfeiting of the state's seal or currency, falsification of official documents, perjury before consular officials, and conspiracy to violate immigration or customs laws."[64]

An FDPR targeting military products sent to a specific military end user would fall squarely within Category (e)—but an FDPR encompassing purely commercial products (an iPhone, Laptop, or car) sold to a commercial enterprise (such as a supplier of consumer products or computers) is far more questionable.

Most U.S. trade agreements prohibit trade restrictions except where necessary to protect national security. For example, the General Agreement on Tariffs and Trade (GATT) prohibits most trade restrictions but permits parties to the agreement to take "any action ***which it considers necessary for the protection of its essential security interests***" such as restricting trade of "fissionable materials" or "implements of war."[65]

Similar "national security" exemptions are included in most U.S. trade agreements.[66]

---

59 RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (A. L.I. 2018).

60 Aside from Category (b), it is plain on its face why the other categories would not cover extraterritorial assertions of jurisdiction to protect either national security or the U.S.'s commercial interests. Category (b), the "substantial effects" doctrine, would require a "direct, substantial, and reasonably foreseeable" link between the action regulated and some effect on the U.S., (*see* RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 409, rep. n. ¶ 2) and the very attenuated and speculative causal chains covered under the FDPR do not fulfill this requirement.

61 *Understanding the Extraterritoriality of U.S. Export Controls, supra* note 16.

62 *Id.*

63 RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (A.L.I. 2018).

64 RESTATEMENT (FOURTH) FOREIGN RELATIONS LAW OF THE UNITED STATES § 412 (A.L.I. 2018).

65 GATT, *supra* note 18, art. XXI (emphasis added).

66 Kartikeya Garg, *The National Security Exception in International Trade and Cybersecurity*, 2 COMMONWEALTH CYBER J. 110, 120–25, (2024).

Therefore, while both international jurisdiction limits and trade agreements permit allow a narrow FDPR blocking sales of military equipment to military end users, a sweeping FDPR blocking sales of old iPhones or laptops to non-military user is harder to defend.

2. The expanding FDPR pushes the concept of "good faith" national security to uncharted territory

Security exemptions to otherwise applicable international laws (such as jurisdictional constraints or treaties) strongly defer to states' own interpretations of national security. International courts rarely second-guess whether a particular measure is necessary to protect a state's essential security interests.[67]

However, while international courts avoid second-guessing nations' *judgments* about their own national security interests, they can and do review whether such "national security" claims are made in *good faith*.[68] Recently, in a dispute before the World Trade Organization (WTO) between Ukraine and Russia, Russia cited national security interests to justify imposing travel restrictions.[69] While acknowledging that it is "left, in general, to every Member to define what it considers to be its essential security interests[,]"[70] the panel cautioned that members are *not* "free to elevate any concern to that of an 'essential security interest.'"[71] Members must only cite "national security" interests when they have a "good faith" belief that such actions further national security interests: states should not to "circumvent their obligations" under international treaties by "relabeling trade interests" as national security interests.[72]

The Entity List Rule may have started as a good faith effort to target a specific entity deemed to threaten U.S. national security (Huawei). However, it has expanded to prohibit worldwide sales of consumer goods to hundreds of commercial companies—appearing far more like a pretext for protectionist trade policies.

Insufficient tailoring of the Rule and the U.S.'s willingness to suspend rules in exchange for non-security-based economic concessions suggest the U.S. is using the FDPR as an economic tool, rather than in a good-faith effort to protect national security.

a) Insufficient tailoring undercuts a good faith rationale

International law would likely defer to the FDPR rules that identify and control specific items as national security threats, even when the controls apply to

---

67 Fabian Eichberger, *Self-judgment in international law: Between judicialization and pushback*, 37 LEIDEN J. OF INT'L L. 915 (2024).

68 Measures Concerning Traffic in Transit Report, *supra* note 19, ¶¶ 7.132–7.138.

69 *Id.*, ¶ 7.22.

70 *Id.,* ¶ 7.131.

71 *Id.,* ¶ 7.132.

72 *Id.*, ¶¶ 7.132–7.138.

a broad swath of end users. The ability to self-identify which items pose threats to national security interests likely falls within nations' "general" authority to identify such interests and therefore, does not violate international law.[73]

However, FDPR fn1,4,5 imposes no end-product requirements of any kind, controlling *non-security* items. The U.S. has clarified that the recent additions to the FDPR indicate that FDPR fn1,4,5 captures "foreign-produced EAR99 [non-restricted] items that are a direct product of non-U.S.-origin technology or software that is not subject to the EAR."[74] The covered technology is multiple degrees of separation from the technology that was actually identified as posing a security risk. Neither the covered technology nor the machine used to make it have been identified as a security risk. Instead, the product is covered simply because the machine used to make the machine that made the product *was* covered.

This causal chain has no limit, and the U.S. government has telegraphed an intent to enforce these rules vigorously. The U.S. has sent Compliance notices to foreign institutions, warning them that they may become "the next example of U.S. enforcement against a foreign party" if they do not tread carefully.[75] The government further asserts that "BIS [Bureau of Industry and Security] actively enforces U.S. export control laws, regardless of where the offending party is located. Anyone involved in the movement of items subject to the EAR must adhere to U.S. export control laws."[76] For example, the U.S. government brought an export enforcement action against Seagate,[77] an international company incorporated in Ireland.[78] Seagate exported machines to overseas factories in Singapore.[79] The machines were classified as ECCN 3B992, not independently subject to the FDPR rule.[80] However, because the machines *themselves* were a direct product of ECCN 3E991 technology, which *is* included in the list of FDPR covered products, the FDPR did apply to the machines as a "direct product" of

73 *Id.,* ¶ 7.131.

74 *Foreign-Produced Direct Product (FDP) Rule as it Relates to the Entity List* §§ 734.9, 736.2(b)(3), and footnote 1 to Supplement No. 4 to pt. 744, BUREAU OF INDUS. AND SEC. (Mar. 31, 2022), https://perma.cc/PYG7-Q863.

75 Olga Torres & Derrick Kyle, *U.S. Government to Foreign Persons: Comply with Economic Sanctions and Export Control Laws*, TORRES TRADE L. (Mar. 7, 2024), https://perma.cc/7SRH-63D3.

76 *Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note: Obligations of foreign-based persons to comply with U.S. sanctions and export control laws,* 5 (Mar. 6, 2024), https://perma.cc/77X4-C9UD [hereinafter *Tri-Seal Compliance Note*].

77 *BIS Imposes $300 Million Penalty Against Seagate Technology LLC Related To Shipments To Huawei*, BUREAU OF INDUS. AND SEC., (Apr. 19, 2023), https://perma.cc/ZNW4-X9AK.

78 *Seagate Fiscal Year Annual Report*, SEAGATE (2021), https://perma.cc/S456-9J5N.

79 Sussman, *Seagate*, *supra* note 2.

80 *Id.*

controlled technology.[81] The initial export of the machines was permissible as the machines went to Singapore, which is not a country or entity that the U.S. government has identified as posing a security risk.[82] In Singapore, Seagate used the machines to coat surfaces of HDDs (Hard Disk Drives).[83] Seagate then sold the HDDs to Huawei, which is on the entity list.[84] Seagate's HDDs were classified as EAR99s (so generally NOT subject to specific export rules).[85] However, because the not-otherwise-covered HDDs were made using machines that had been made using covered technology, shipping the HDDs to Huawei was impermissible under the FDPR Entity List provision.[86]

This sequence of events exemplifies the absurdity of claiming this rule legitimately covers only "national security" interests. In today's connected world of "the Internet of Things," *anything* can be swept up in the FDPR even if it is only very tangentially connected to an item about which the U.S. government has identified national security concerns. A "tainting" effect occurs when a controlled product is used to manufacture other items: "the mere fact that a machine, itself subject to an U.S. export license, constitutes a major component of the factory producing the products, in effect taints all products it touches."[87]

This rule's text would not, in theory, prevent it from being applied to bar the sale of a French-made consumer-grade robot vacuum used to clean floors to a commercial business such as Inspur Electronics[88] (the "Hewlett Packard" of China) or another "entity list" item, if that robot vacuum contained integrated circuits or semiconductors[89] (even low-grade integrated circuits) that were made in a factory which was, in turn, made using controlled U.S. technology.[90] No portion of the rule provides an exception when the end-product is low-tech and non-covered—or even for old, obsolete products. The rule purports to cover a ten-year-old desktop sitting in a junkyard, with a stated justification of U.S. "national security." Applied to such extremes, such a rationale is patently absurd.

81 *Id.*

82 *Id.*

83 *Id.*

84 *Id.*

85 *Id.*

86 *Id.*

87 *Id.*

88 Entity List, *supra* note 11, at 538.

89 Even Roombas contain several—*see* Kenny Shi et al., *Disassembly and Analysis of iRobot Roomba 565*, REC FOUNDATION (2023) https://perma.cc/423A-LAN3.

90 For example—Footnote 1's "input" criteria (15 C.F.R. § 734.9(e)(1)(i)(B)) covers items which are the "product of a complete plant or 'major component' of a plant that is a direct product" of technology classified under ECCN 3D001. ECCN 3D001 includes software used to produce commodities classified as ECCN 3A090—integrated circuits.

If the implicated products did implicate national security, or if the administrations limiting their movement believed they did, such items could easily be included on the restricted items list. Poor draftsmanship or overly conservative judgments about which products may be dangerous would generally benefit from deference to the U.S. government's judgment. But these products are sold worldwide without restriction, belying any national security concern. That many implicated items are not listed suggests that even the limiting regulators admit the sale of such items does not threaten national security at all.

A rule that necessarily captures plainly non-security goods may have made sense when the rule was intended to be applied only to a small subset of military-end users. The U.S.'s judgment that, for example, selling *any* useful products of *any* kind to a Beijing-based missile manufacturer threatens U.S. national security would likely pass a "good faith" test in the national security context. However, the entity lists now includes hundreds of nonmilitary companies and the list continues to expand[91]—and with the Affiliates Rule, would extend to thousands of companies worldwide, even in allied nations.[92]

Although the stated reason for including non-military end-users is diversion concerns, the Affiliates Rule is both too broad and too narrow to address diversion. The rule is too broad because it *would* include a company with 50% U.K. ownership with the remaining 50% of ownership split evenly between fifty different companies on the Entity List.[93] Such a company is not meaningfully controlled by any Entity List company, yet, the Affiliates Rule would add it to the Entity List even without any indication of product diversion.[94] On the other hand, the rule would *not* cover a company which is 49% owned by a single company on the Entity List, with the remaining 51% of ownership divided between hundreds or thousands of shareholders,[95] a structure much more likely to result in diversion.

Even more tellingly, the U.S. government has compromised on the Affiliates Rule in exchange for economic—not national security based—concessions.

b) Use of the Entity List as a bargaining tool in economic dealmaking undercuts the government's argument that the entity list protects national security

The Trump Administration agreed to suspend the entire Affiliates Rule in exchange for China agreeing to halt rare earth metal export constraints.[96] This

91 Entity List, *supra* note 11, at 538.

92 Nat'l Foreign Trade Council, Comment Letter on Interim Final Rule "Expansion of End-User Controls to Cover Affiliates of Certain Listed Entities" (Oct. 29, 2025), https://perma.cc/R362-B9ZD.

93 Affiliates Rule, *supra* note 13.

94 *Id.*

95 *Id.*

96 Chiacu & Alper, *supra* note 15.

negotiation pattern does not treat the Affiliates Rule as a critical, must-have restraint on trade to protect national security, but rather as a bargaining chip in an economic trade war.

Suspending the Affiliates Rule for a year in exchange for trade concessions suggests instead that the executive branch does not in fact perceive the Affiliates Rule as necessary to protect national security. Rather, the Executive understands these restrictions to be a bargaining tool to improve the U.S.'s economic negotiating position, a matter of economic policy, not national security. This conduct strongly suggests the U.S. government's use of the "national security" justification is in bad faith, a pretext for the true economic motive for imposing such regulations, which violates international law.

B. The best reading of the Export Control Act of 2018 (ECRA) aligns with international law and therefore does not permit a standardless expansion of the FDPR

The ECRA provides the domestic law authority for the executive branch to impose export controls.[97] The best reading of this statute under the *Charming Betsy* canon of interpretation, the ECRA text, the nondelegation doctrine, and intelligible principle test would limit the Executive's authority to enact any regulations that violate international law.

U.S. law recognizes the *Charming Betsy* canon, which provides that when a statute is susceptible to more than one interpretation—one that would violate international law and one that would not—courts should adopt the interpretation that avoids the conflict.[98] However, the U.S. Congress retains the ability to overrule international law.[99] If a statute explicitly violates international law, then U.S. law controls.[100] Parties objecting to the violation of international law may seek international, but not domestic, recourse.

ECRA certainly *can* be read to comply with international law. Although it clearly applies extraterritorially[101] as it specifies that its regulations apply to "foreign persons,"[102] the statute can easily be read to permit extraterritorial exercises of jurisdiction only where permitted by international law.

---

97 50 U.S.C. §§ 4811–4826, *supra* note *22*.

98 Murray v. The Schooner Charming Betsey, 6 U.S. 64, 118 (1804).

99 Frederic L. Kirgis, *International Agreements and U.S. Law*, 2 ASIL INSIGHTS (May 27, 1997), https://perma.cc/8R8L-T8FE.

100 *Id.*

101 Overcoming the typical "presumption against extraterritoriality." *See* Morrison v. National Australia Bank Ltd., 561 U.S. 247, 255 (2010).

102 50 U.S.C. § 4812(a)(1), (b)(1).

Such a reading of the statute is also most closely aligned with the statute's text. ECRA allows the U.S. President to control "the export, reexport, and in-country transfer of items ***subject to the jurisdiction of the United States***, whether by United States persons or by foreign persons."[103] Notably, ECRA restricted export controls to items that were *already* "subject to the jurisdiction of the United States"—it did not purport to *expand* that jurisdiction, nor did it include the jurisdictional hooks that Commerce would include in the new FRPR fn. 1,4,5 rules.

Furthermore, Section 4813(a)(2), the statutory basis for the creation of the Entity List in specific[104] directs that the List to be created to: "control the release of items" used for "weapons," "terrorism," "military programs," or "interference with or disruption of critical infrastructure."[105] This list aligns very closely with the kind of activity which might reasonably be regulated under the "protective principle," and does not indicate any intent to overrule international law. Reading ECRA to align with international law, the statute grants the executive branch the authority only to impose controls as needed to protect national security. If so, any regulations that do not have a good faith national security basis exceed ECRA's grant of authority.

ECRA also disfavors "unilateral export controls" (of any kind) and instructs that unilateral controls "should be limited for purposes of protecting specific United States national security and foreign policy interests."[106] Unilateral export controls imposed against a narrow list of dangerous entities or which cover a discrete list of dangerous products meets this standard—but diffuse bans on consumer goods to thousands of companies does not.

Finally, ECRA indicates that, before enacting any controls, the Executive should consider whether the proposed controls will harm the U.S.'s ability to maintain its "leadership in the science, technology, engineering, and manufacturing sectors," as well as the U.S.'s "competitive[ness] in the global markets."[107] A broad FDPR stands to harm U.S. "leadership" and "competitive[ness]" in global markets for technology, both by arbitrarily limiting the sale of certain products which do not themselves pose any national security risk and by increasing the burdens associated with using U.S. products.

Under this scheme, entities considering buying from the U.S. or using U.S. technologies will have to remember and weigh the possibility that innocuous items will without warning be subjected to intense U.S. export regulations, sometimes years after the technology shipped. The FDPR fn.1,4,5 provision shows no

103 50 U.S.C. § 103 (emphasis added).

104 50 U.S.C. § 4813(a)(2).

105 50 U.S.C. § 4811(2)(A).

106 50 U.S.C. § 4811.

107 50 U.S.C. § 4811(3).

consideration at all for the harm it will cause to U.S. business interests, ignoring ECRA's requirement that such regulations weigh such considerations. The FDPR fn. 1,4,5 also demonstrates only a thin connection to the statutory authority permitting export controls.

The canon of statutory interpretation based on the nondelegation doctrine, which assumes that Congress would not grant expansive authority to administrative agencies without any intelligible limiting principle,[108] also supports this interpretation of ECRA. As ECRA does not explicitly authorize the Executive to impose export controls that violate international law or that are not necessary to protect national security. it should not be read as allowing BIS to impose any and every extraterritorial export control anywhere, for any reason, over anything.

In today's Internet-of-Things World, the FDPR now purports to encompass nearly every foreign product that includes a semiconductor or software—a sweeping jurisdictional expansion that should not have taken place in footnotes in a regulation. If Congress intended to seize jurisdiction over nearly all foreign-designed and foreign-made products, it should have said so expressly.

IV. Available Recourse—The Limits of Pathways to Challenge the FDPR

A. Even as the FDPR Expands, Enforcing International Law in an International Forum is Unlikely to Succeed

On a practical level, an international forum with both the jurisdiction and the political might to enter a judgment against the U.S. and enforce it does not currently exist.

The International Court of Justice (I.C.J.) has heard complaints about violations of sovereignty,[109] which would make it an appropriate forum to hear an impacted country's claim that the U.S.'s expanded FDPR violated its sovereignty.

However, without consent from the U.S., which is very unlikely in the current political climate, no case can be brought before the I.C.J.. While the U.S. previously agreed to the I.C.J.'s compulsory jurisdiction, the U.S. has since withdrawn from the provision which provided the I.C.J. with Compulsory Jurisdiction over disputes involving the U.S.[110] in response to the I.C.J.'s handling

---

108 *Cf.* Indus. Union Dept. v. Amer. Petroleum Inst., 448 U.S. 607 (1980); Gundy v. United States, 558 U.S. (2019) (both reading limiting principles into a statute to bring it into compliance with the nondelegation doctrine).

109 Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (June 27).

110 Statement By the U.S. Dep't of State (Jan. 18, 1985) https://perma.cc/A3W8-2JQE.

of a case in which Nicaragua alleged the U.S. had violated its sovereignty.[111] None of the treaties to which the U.S. is a party that provide for mandatory I.C.J. jurisdiction over disputes apply to this particular matter. Therefore, the I.C.J. would not have jurisdiction to hear a claim that the U.S. has violated other nations' sovereignty through FDPR fn.1,4,5 unless the U.S. consented to such a case.

Politically, nothing suggests that the U.S. would make such a concession and permit a case involving it to come before the I.C.J.. Indeed, the U.S. has expressed the view that international bodies such as the WTO should not review or second-guess a state's claim that its action is necessary for national security,.[112] Therefore, while the I.C.J. could in theory preside over such a case, in practice, unless the U.S. dramatically shifts policy, it will not accept I.C.J. jurisdiction. Perhaps a nation with something extremely desirable to offer the U.S. could successfully negotiate for the U.S. to consent to jurisdiction in a particular case, but so far, no such deals have manifested or appeared on the horizon.

The WTO has a mandatory dispute resolution organ which would have the authority to preside over a claim that the U.S. has violated the WTO Agreement. This same body reviewed Ukraine's claim[113] that Russia had violated the WTO Agreement and weighed Russia's assertion of national security interests. Unlike the I.C.J., formally, the U.S. does not have the ability to decline to consent to the WTO's dispute resolution organ: because the U.S. is a party to the WTO Agreement, it is bound by the dispute organ.[114]

However, this route is similarly nonviable due to the crumbling enforcement mechanism within the WTO.[115] Any party unhappy with a decision from the Dispute Settlement Body (DSB) at the WTO can appeal that decision, and, when appealed, the DSB's decisions are automatically stayed pending resolution of the appeal by the Appellate Body at the WTO.[116]

Unfortunately, the U.S. has decimated the efficacy of the WTO's Dispute Resolution Mechanism. In recent years, the U.S. has consistently refused to permit any judicial appointments at the Appellate Body of the WTO Dispute Resolution

111 Nicar. v. U.S.*,* 1986 I.C.J. at 146–150; Farooq Hassan, *A Legal Analysis of the United States' Attempted Withdrawal from the Jurisdiction of the World Court in the Proceedings Initiated by Nicaragua*, 10 U. DAYTON L. REV. 295, 295 (1984).

112 Measures Concerning Traffic in Transit Report, *supra* note 19, ¶¶ 7.51–7.53.

113 *Id.*

114 Understanding on Rules and Procedures Governing the Settlement of Disputes Article 1.1, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 2, 1869 U.N.T.S. 401; *Introduction to the WTO dispute settlement system*, WORLD TRADE ORG., https://perma.cc/6P2D-5S6Y, (last visited May 15, 2026).

115 Kristen Hopewell, *Unravelling of the trade legal order: enforcement, defection and the crisis of the WTO dispute settlement system*, 101 INT'L AFFS. 1103, 1104 (2025).

116 *Id.*

Mechanism.[117] The Appellate Body cannot issue any decisions without new judicial appointments, so pending appeals are never resolved by the non-existent Appellate Body.[118] The temporary stay of the DSB's decisions are now de facto permanent stays.[119] Therefore, any party who receives an adverse decision from the DSB can undo that decision in perpetuity by filing an appeal. Unless and until the U.S. agrees to allow the appointment of judges to the Appellate Body, WTO action will likely prove fruitless.

B. Enforcing International Law in a National Forum is Likely to Fail

At present, there is no legal basis for a foreign state to sue in domestic court asserting that the U.S. violated the customary rules of international sovereignty. Sovereign immunity protects the U.S. government against such a suit unless the U.S. government expressly consents.[120]

While the U.S. has adopted the WTO Agreements as binding law,[121] affected companies, countries, or individuals both within the U.S. and outside of the U.S. still cannot bring suit in U.S. domestic courts over violations of the WTO Agreements. The *Uruguay Round Agreements Act*, which adopted the WTO Agreements, explicitly does not permit any individual or entity to challenge the action of a U.S. government agency under the Act.[122] Instead, only the federal government may sue to enforce the WTO Agreement if more local entities (such as state governments) take actions that the federal government understands to violate the WTO Agreement.[123]

Therefore, suits brought in U.S. domestic courts under international bases of law are likely futile for both international state actors and private actors affected by the regulations in question.

---

117 *Id.*

118 *Id.*

119 *Id.*

120 *Cf.* Principality of Monaco v. Mississippi, 292 U.S. 313, 330 (1934) (holding that U.S. courts have no jurisdiction over suits by foreign governments against a U.S. state unless the U.S. state consents); United States v. Clarke, 33 U.S. 46 (1834) ("As the United States are not suable of common right, the party who institutes such suit must bring his case within the authority of some act of congress, or the court cannot exercise jurisdiction over it.").

121 Uruguay Round Agreements Act, Pub. L. No. 103-465,108 Stat. 4809 (codified in scattered sections of 19 U.S.C.).

122 19 U.S.C. § 3512(c).

123 *Id.*

C. Recourse Under Domestic Law is Limited

Relief in U.S. courts, under U.S. law, would also be a long shot. U.S. courts are, in general, exceedingly sympathetic to and solicitous of actions by the executive branch which were done under the banner of "national security,"[124] and the possible avenues of relief available here are limited.

While the presumption against extraterritoriality is of no concern within the context of the statute and associated regulations, there is a legitimate argument—albeit one which courts are likely to view with hesitance—that the FDPR fn.1,4,5 exceeds the Executive's statutory authority. If that argument fails, even more difficult—and narrow—relief may exist under the nondelegation doctrine or the APA.

1. An *ultra vires* claim is possible, but difficult

Perhaps the most viable claim to bring in U.S. courts is an *ultra vires* challenge alleging that the Entity List provisions of the FDPR exceed the executive branch's statutory authority.[125] *Ultra vires* claims are not precluded under ECRA.[126]

However, prevailing on any *ultra vires* claim is very difficult: the plaintiff must establish that "(i) there is no express statutory preclusion of all judicial review; (ii) there is no alternative procedure for review of the statutory claim; and (iii) the agency plainly acts in excess of its delegated powers and contrary to a specific prohibition in the statute that is clear and mandatory."[127] The D.C. Circuit, in a case involving other provisions of ECRA, emphasized that prevailing on an *ultra vires* claim would likely be very difficult.[128]

Ultra vires claims involving ECRA and the FDPR are rare, but the D.C. Circuit[129] has considered an *ultra vires* claim to an Entity List addition once—albeit on a preliminary injunction appeal and not on the case's merits.[130] There, the Circuit construed ECRA extremely broadly, suggesting that the free-floating

---

124 Shirin Sinnar, *Courts Have Been Hiding Behind National Security for Too Long*, BRENNAN CENTER FOR JUSTICE (Aug. 11, 2021), https://perma.cc/C3TA-EVZN.

125 *Cf.* Leedom v. Kyne, 358 U.S. 184 (1958).

126 *See* Fed. Express Corp. v. United States Dep't of Com., 486 F. Supp. 3d 69, 79 (D.D.C. 2020) (noting that while the *ultra vires* claim failed in that case, "Congress cannot be 'understood [even] generally to have precluded [judicial] review'—let alone ultra vires review").

127 5 U.S.C. § 706.

128 *See* Federal Express Corp v. Dept. of Commerce, 39 F.4th 756, 764 (D.C. Cir. 2022) ("[U]ltra vires claims are confined to extreme agency error where the agency has stepped so plainly beyond the bounds of [its statutory authority], or acted so clearly in defiance of it, as to warrant the immediate intervention of an equity court.") (internal quotation marks omitted); *see also id.* at 765 (referring to *ultra vires* claims as a "Hail Mary" pass).

129 No other circuits appear to have considered a similar case.

130 Changji Esquel Textile Co. v. Raimondo, 40 F.4th 716 (D.C. Cir. 2022).

ECRA provision permitting the Secretary to "undertake any other action as is necessary to carry out this subchapter that is not otherwise prohibited by law" allowed for broader additions to the Entity List.[131] On its face, this is a poor construction of the statute and should be overturned; the statute granting authority to the Secretary to create the Entity List points only to national security bases[132] and no others for adding entities to the list.

However, even if other circuits are reluctant to directly contradict or overturn *Changji Esquel Textile Co. v. Raimondo*,[133] the legal question presented there (whether human rights abusers can be added to the Entity List) is distinct from any question regarding implementing economic policy through the FDPR and can be distinguished.

First, in the context of human rights abuses—but not economic policy—there may be another basis for asserting extraterritorial jurisdiction that is in compliance with international law[134]: addressing offenses of "universal concern" can be a basis for extraterritorial assertions of extraterritorial jurisdiction,[135] and so the *Charming Betsy* canon would not necessarily be relevant. Second, the textual issues which suggest that the authority for broad economic embargos is *not* provided under ECRA also do not apply—or apply less—to targeted prohibitions against sales to specific entities identified as human rights violators. Such a restraint is "limited" in pursuit of a "specific" goal[136] and does not imperil the U.S.'s economic "competitiveness"[137] in an undue or unconsidered manner. Furthermore, in contrast with economic considerations, "the protection of human rights" *is* explicitly listed as one of ECRA's purposes[138] (albeit not in the section providing the basis for the creation of the Entity List). Finally, in the context of the nondelegation doctrine, construing the statutory provision permitting "any other action as is necessary to carry out this subchapter" to narrowly include legal actions taken to (1) protect national security and (2) prevent human rights abuses is an odd construction of the statute, but does at least reads intelligible limiting principles into the statute.

---

131 *Id.* at 723.

132 50 U.S.C. § 4811(2)(A).

133 40 F.4th 716.

134 Whether this argument would or would not comply with international law is outside of this Comment's scope, but the doctrine at least provides another colorable claim of conformity with international law in the Changji v. Raimondo case.

135 RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (A. L.I. 2018).

136 50 U.S.C. § 4811(6).

137 50 U.S.C. § 4811(3).

138 50 U.S.C. § 4811(2)(D).

Expanding the *Changji Esquel Textile Co. v. Raimondo*[139] ruling and reading this section of the statute to permit *any action by the Secretary that could be considered "foreign policy"*—as long as it is not *explicitly illegal*—provides no limiting principle whatsoever and would implicate the nondelegation doctrine.

2. Narrow avenues for relief in the event that an *ultra vires* claim is not viable

If courts instead elect to construe ECRA extremely broadly, to allow the executive branch to impose any extraterritorial export controls for any reason—or no reason—at all, affected parties could raise constitutional arguments that the underlying statute violates the nondelegation doctrine.[140] While invalidations of statutes are rare—and the intelligible principle test[141] sets a low bar for statutes to clear—the Executive's interpretation of ECRA increasingly casts it as providing virtually limitless authority over huge swaths of economic regulation to BIS. If the courts agree with that reading of the statute, it may be a significant enough delegation of power to implicate the doctrine.

Relief under the APA[142] for agency action that is arbitrary, capricious, or in excess of the agency's statutory authority under ECRA is limited[143] but not non-existent. Civil penalties and administrative sanctions (including the "suspension or revocation" of authority to export) are "subject to judicial review."[144] While such challenges would be limited in scope, affected parties could challenge particular enforcement actions surrounding the Entity List Rule as applied to them.

If the U.S. government continues to push the boundaries of this rule further, as it has indicated it may, a severely impacted U.S. company might be able to bring a regulatory takings claim under the Fifth Amendment.[145] On its face, such a claim would provide only very limited relief in the form of compensation. It could, however, influence U.S. policy by making regulatory takings claims appear less attractive to the U.S. government, ultimately encouraging a more nuanced approach to what products actually must be restricted.

139 40 F.4th 716.

140 *See generally* Federal Communications et al. v. Consumers' Research et al., 606 U.S. 656 (2025) (discussing and applying the intelligible principle test in a nondelegation doctrine claim).

141 *Id.*

142 *See* Fed. Express Corp. v. United States Dep't of Com., 486 F. Supp. 3d. 79 (noting that while the *ultra vires* claim failed in that case, "Congress cannot be 'understood [even] generally to have precluded [judicial] review'—let alone ultra vires review").

143 50 U.S.C. § 4821(a).

144 50 U.S.C. § 4843(c).

145 Penn Central Transportation Co. v. New York City, 438 U.S. 104, 124 (1978).

However, such a claim is almost certainly not ripe yet and may never be ripe. The *Penn Central* factors for partial regulatory takings typically consider (1) economic impact, (2) investment-backed expectations, and (3) the character of the regulation, and sometimes factors into the analysis (4) the reciprocity of advantage to the regulated party.[146] Whether a company would prevail on these factors would be a fact-specific inquiry dependent on that company's specific situation, but doing so is generally quite difficult, especially in areas—like national security—where courts are hesitant to intrude.

D. U.S. Governmental Action

Even if the U.S. government does not anticipate receiving a judgment invalidating the portions of the FDPR fn.1,4,5 or anticipates that it will be able to avoid complying with any judgment they do receive, out of pure self-interested concerns, the U.S. government can and should independently enact policy changes to limit the FDPR so it covers only good faith national security concerns, and resist the temptation to use it as an economic tool.

Maintaining the U.S.'s current ever-broadening approach to extraterritorial export controls risks prompting similar behavior from other nations, harming the U.S. economy, and undermining the U.S.'s reputation on the global stage.

1. The potential for retaliatory export controls

When U.S. regulation blurs the line between economic policy and national security policy,[147] it complicates foreign relations dilemmas[148] and encourages other nations to enact similar measures. China has already begun to engage in retaliatory export constraints.[149] Other countries may follow suit.

If these rules proliferate across numerous states, without any limiting principle such as a clear-cut and narrowly delineated national security basis, we may ultimately live in a world in which a plethora of rules from multiple nations apply to a particular product, enormously burdening the legal system, innovation, and trade. This bold application of U.S. law functions effectively only if no other nations impose similarly burdensome rules. That gamble seems risky, particularly

146 *Id.* at 123–28.

147 Stephen Kho and Yujin McNamara, *Focus on China: The Expansive Use of National Security Measures to Address Economic Competitiveness Concerns*, 17 U. PA. ASIAN L. REV. 368 (2022).

148 Rachel Brewster, *Border and Boundary: A New Global Corporate Regulatory Power?: Market Entry as the for Prescriptive Jurisdiction*, 59 U. CHI. LEGAL F. 59, 70–76 (2023).

149 Xinghui Kok, *US, China talks sketch out rare earths, tariff pause for Trump and Xi to consider*, REUTERS (Oct. 26, 2025), https://perma.cc/477J-ZK28.

as the U.S. continues to undermine its relationships with foreign governments through hostile commentary and actions.[150]

2. Harm to the U.S. Economy

This new iteration of the FDPR risks devaluing U.S. goods. Any owner of a factory built with U.S. technology now resign themselves to the fact that at any moment, the U.S. government could substantially hinder their business with a new restraint on where and to whom they may sell their products, even if they produce low-risk, low-tech, previously unregulated products.

Companies facing an increased risk that the U.S. will impose burdensome regulatory requirements in violation of international law may deem it wise to cease reliance on U.S. technologies to shield themselves from potential liability. This liability is nontrivial. The DOJ asserts that they have the authority under the International Emergency Economic Powers Act (IEEPA) and ECRA to bring criminal prosecutions against individuals who violate export control laws.[151] These rules permit bringing civil or criminal indictments, including against foreign entities, for "causing a violation of any license, order, regulation, or prohibition issued" pursuant to IEEPA as well as "causing" or "inducing" the doing of any act prohibited or the omission of any act required by the ECRA or EAR.[152]

Penalties for noncompliance (including as a foreign user)[153] can include heavy fines, "loss of ability to trade in U.S.-controlled goods, and imprisonment, including up to 20 years for willful noncompliance.[154] For example, after the U.S. government sued Seagate for selling HDDs to Huawei, Seagate ultimately settled for the "largest standalone administrative penalty in BIS history": nearly $300 million in penalties.[155]

Even a company which feels confident it can perfectly comply with these U.S. restrictions would still have good reason to be leery of continuing to use U.S technology. Substantial impediments to a company's ability to sell products produced using equipment manufactured with U.S. technology would abruptly diminish that equipment's value.

As such, foreign businesses are likely to begin to shift away from using U.S. technologies if this overexpansive reach and unpredictability persists, harming U.S. businesses and ultimately diminishing the U.S. government's ability to curtail

150 Margaret McMillan, *Making America Alone Again*, FOREIGN AFFS. (July 21, 2025), https://perma.cc/CS74-W7P9.

151 Torres and Kyle, *supra* note 75; *Tri-Seal Compliance Note*, *supra* note 76.

152 *See* 50 U.S.C. § 1705(c); 50 U.S.C. § 4819(b); *Tri-Seal Compliance Note*, *supra* note 76, at 7.

153 *Understanding the Extraterritoriality of U.S. Export Controls*, *supra* note 16.

154 *Tri-Seal Compliance Note*, *supra* note 76, at 8.

155 *Id.* at 7.

the dispersal of critical products through targeted rules because the U.S.'s sphere of economic influence will dwindle.

Currently, the U.S. scores very high in innovation metrics,[156] producing many highly desirable technologies. It is possible that, at least for a while, foreign manufacturers and entities will deem at least some U.S. technology sufficiently high-quality to merit dealing with burdensome and unpredictable regulations. However, over time, there is no reason at all that other countries, particularly wealthy countries with developed economies like China, cannot invest in innovation, education and technological development and ultimately reduce their reliance on U.S. technologies.

3. Drains on U.S. Credibility

Finally, imposing unreasonable rules which conflict with international legal standards regarding extraterritoriality may harm the U.S.'s credibility on an international scale. Even when countries cannot, in the short term, be forced to comply with international law, consistent violations have long-term consequences: reputations erode, bargaining power diminishes, and other countries become less likely to respect international law in response.[157]

Furthermore, while the U.S. has currently been successful in imposing these rules on foreign nationals, it is entirely possible that, should the U.S. push its authority too far, foreign nationals will cease to treat the FDPR as a legitimate basis of law and refuse to comply with judgements based on it. While the U.S. might be able to force the issue in some cases, such as by seizing property within the U.S., if a foreign national already has all the U.S. technology they want (for example, if they have already constructed a factory outside of the U.S. and wish only to produce HDDs and sell them as they please) and have no property within U.S. reach, it might be difficult for the U.S. to enforce such a ruling without local recognition that the rule is legitimate. Such an enforcement dilemma would undermine the U.S.'s image on the international plane.

V. CONCLUSION

At present, the U.S. enjoys a powerful position: industry in many other countries rely on U.S. technologies to manufacture a wide range of products and technologies. However, such power should be exercised lawfully in compliance with both domestic and international law. Overreaching, illegal, and unjustifiable regulation of U.S. technology after it is lawfully sold abroad risks pushing people in other nations to turn elsewhere for reliable innovation. Far from benefitting national security, such a shift would damage both U.S. industry and national

---

156 *United States of America ranking in the Global Innovation Index 2025*, WORLD INTELL. PROP. ORG., https://perma.cc/WH9S-TS5J (last visited Jan. 29, 2026).

157 Shai Dothan, *Violating International Law Is Contagious*, 23 CHI. J. INT'L L. 79 (2022).

security. Currently, the U.S. enjoys the ability to effectively curtail many sales of genuinely dangerous or sensitive technology because so much of this technology flows from U.S. companies. If the locus of investment and innovation shifts due to an increasing sense that U.S. products might carry with them hidden and unpredictable regulations, the U.S. may eventually find itself entirely outside of and unable to regulate the flow of cutting-edge technology at all.

The FDPR, in principle, is both internationally and domestically legal and based on reasonable public policy interests. However, extending the FDPR without reasonable, well-defined limits so it can include not only products significant to national security but also products which are only tangentially related to national security is both ill-advised in terms of public policy and violates the law.

The U.S. should return to a version of the FDPR that more closely resembles the version which existed from 1959–2020 by narrowly tailoring the rule to address only genuine national security concerns. To the extent possible in international and domestic forums, foreign governments and U.S. companies should bring challenges pressuring the U.S. government to make this change, but even in the absence of such challenges, the U.S. government should consider taking such action of its own accord to preserve domestic and foreign U.S. interests. In general, the Rule should only apply to products which are themselves flagged as national security concerns, not only those *made with* products which represent national security concerns, and any restrictions on sales of consumer goods to specific, potentially dangerous, entities should be extremely narrowly targeted. It is also worth carefully considering which products merit their designation as national security concerns and those which do not—and might instead have earned their place on the list unfairly due to economic rather than security concerns.